AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

[H.A.S.C. No. 110–50]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2008

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED TENTH CONGRESS

FIRST SESSION

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE HEARING

ON

BUDGET REQUEST ON INFORMATION TECHNOLOGY

HEARING HELD
MARCH 28, 2007

U.S. GOVERNMENT PRINTING OFFICE

43–956 WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

ADAM SMITH, Washington, *Chairman*

MIKE MCINTYRE, North Carolina
ROBERT ANDREWS, New Jersey
JIM COOPER, Tennessee
JIM MARSHALL, Georgia
MARK UDALL, Colorado
BRAD ELLSWORTH, Indiana
KIRSTEN GILLIBRAND, New York
KATHY CASTOR, Florida
MAC THORNBERRY, Texas
ROBIN HAYES, North Carolina
KEN CALVERT, California
JOHN KLINE, Minnesota
THELMA DRAKE, Virginia
K. MICHAEL CONAWAY, Texas
JIM SAXTON, New Jersey

BILL NATTER, *Professional Staff Member*
ALEX KUGAJEVSKY, *Professional Staff Member*
ANDREW TABLER, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2007

WEDNESDAY, MARCH 28, 2007

FISCAL YEAR 2008 NATIONAL DEFENSE AUTHORIZATION ACT—BUDGET REQUEST ON INFORMATION TECHNOLOGY

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

FISCAL YEAR 2008 NATIONAL DEFENSE AUTHORIZATION ACT—BUDGET REQUEST ON INFORMATION TECHNOLOGY

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
TERRORISM, UNCONVENTIONAL THREATS AND
CAPABILITIES SUBCOMMITTEE,
Washington, DC, Wednesday, March 28, 2007.

The subcommittee met, pursuant to call, at 2:00 p.m., in room 2122, Rayburn House Office Building, Hon. Adam Smith (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. ADAM SMITH, A REPRESENTATIVE FROM WASHINGTON, CHAIRMAN, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

Mr. SMITH. We will call the meeting formally to order and go ahead and get started.

I appreciate the members and the witnesses, and I look forward to your testimony. I will be brief in my opening comments.

You know we are here today to talk about information technology (IT) within the Department of Defense (DOD), obviously very important issues and multi-layered. And I look forward to the testimony from our two witnesses, in particular how we on this committee can help, because one of our main jurisdictional areas is science and technology in general but information technology in particular, and we want to figure out how we can be as helpful as possible in moving that process forward, and I have looked at your testimony, and I guess the only thing I want to highlight in terms of talking about it is that I think the model is exactly right in terms of, you know, setting up the network, getting people access to it who need access to it to make sure and then protecting it from those who do not. The challenges that I have seen from IT systems, you know, just through the years is that they are great if they work and an utter disaster if they do not, which I realize is not at all helpful, which leads to my question: How do we make sure that we are progressing at the right pace? Because it really comes down to whether or not the people who need to use the system can understand how to use it and if it works for them, you know, whether it is the warfighter, you know, or people in the combatant commands and every step along the way.

Is this something that is going to be user-friendly to them? Is there an adoption period, and it takes a while to figure out? We all understand that, but we are sort of making sure that the system works for the people who have to use it. How can we make sure that we have more successes and fewer failures? Certainly, we

are talking about the specifics of the Navy and Marine Corps Intranet, which is one of the biggest projects in that area, and I know there have been challenges there. So, basically, how we can make sure that we take the right steps so that implementing this information technology works and does not wind up costing us a lot of money to not get the system that we need. I just am curious about your ideas on that.

With that, I will turn it over to Mr. Thornberry for any comments he may have.

STATEMENT OF HON. MAC THORNBERRY, A REPRESENTATIVE FROM TEXAS, RANKING MEMBER, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

Mr. THORNBERRY. Thank you, Mr. Chairman.

I, too, appreciate the witnesses' written testimony, which I have been able to review.

I share your concern. Sometimes you can buy the best widget possible, but the interface between the technology and the human is sometimes where some of the difficulties come. As a country and as a government, we spend a tremendous amount of money on information technology things. Sometimes I think, on one hand, we tend to take it for granted because we all expect it to work, and we have higher and higher expectations of how things will work, and yet, at the same time, it can present enormous vulnerabilities to us, and I know that you both have to look at both sides of it. So I look forward to your oral testimony, and I appreciate your both being here today.

Mr. SMITH. Thank you very much.

With that, we will get started.

We have John Grimes, who is the Assistant Secretary of Defense for Networks and Information Integration and the Chief Information Officer (CIO) for the Department of Defense.

We also have Lieutenant General Charles Croom, United States Air Force, who is the Director of the Defense Information Systems Agency.

Secretary Grimes, we will begin with you.

STATEMENT OF JOHN G. GRIMES, ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION AND CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE

Secretary GRIMES. It is pretty evident that you have a grasp of our problem. So good afternoon, Chairman Smith and Congressman Thornberry, and other distinguished members of the subcommittee. Thanks for the opportunity to testify before the Subcommittee on Terrorism, Unconventional Threats and Capabilities on the importance of information and information technology—and I have made a distinction, "information" and "information technology"—to the overall mission of the Department of Defense.

As you mentioned, I am John Grimes, Assistant Secretary of Defense for Networks and Information Integration, and I am also the Department's CIO. I have provided a written statement for the record. My comments now will focus on how the Department is leveraging information and information technology to rapidly re-

spond to unpredictable, unanticipated and unknown global and national security challenges of today and, hopefully, of tomorrow.

I am sure you are aware of the Department's 2006 QDR, the Quadrennial Defense Review, which recognized Net-Centric technology as a critical part of harnessing the power of information connectivity. It was recognized in this document, which has caused the Department to go into a focus on transformation on Net-Centric operations and activities that will provide a more efficient and effective force. The force includes the warfighter, the Intelligence Community and the business systems that support the warfighter. We call it, or I call it "360." We have touched everything out there, as you indicated, Congressman Thornberry.

The essence of Net-Centric operations is the ability to access information, to share information and to collaborate with others on the Net. To achieve this, we have established four fundamental goals: to effectively build, populate, operate and protect the network. And I think General Croom will elaborate on how we are doing some of that a little bit more, but first, let me explain what I mean when I say, "build, populate, operate, and protect the network."

You may wonder what is he talking about or what does that have to do with defeating the Improvised Explosive Devices (IEDs) in Iraq and so on. It all comes down to one thing, our major focus, which is the sharing of information, of course, on a timely basis. "Building" the network means having IT capabilities and services available to securely move data on the Net, what we call the "transport layer."

"Populating" the Net means that the data and the information is posted on the Net for an authorized user to have access to it any time.

"Operating" the Net means putting in place rules and mechanisms to enable people to access the data and information they need while keeping the Net up and running.

"Protecting" the Net means exactly that—securing the network against cyber attacks and protecting the information on the network and the infrastructure.

Today, the Department operates three IP—Internet protocol—based Intranets. One is unclassified, and two are classified networks. The Department's unclassified network, what we call the Non-classified Internet Protocol Router Network (NIPRNET), is in use by over five million users. This network is connected to the commercial Internet for those agencies doing business with commercial vendors and contractors. The two classified networks are the Department's backbone that work for handling classified information. All of the Intranets operate on a global basis, which is a crucial point.

Information sharing and protection of the network are my two major challenges. We are achieving information sharing through the applications of data standards and a process called the "community of interest." A recent success story is the Maritime Domain Awareness Community of Interest Initiative that the U.S. Navy, the Department of Homeland Security, the Coast Guard, and the Department of Transportation demonstrated. This effort allowed these communities to easily exchange and share daily information

on over 5,000 ships and vessels entering into U.S. coastal areas. What seemed to be a relatively simple thing to do was not until representatives of the various communities agreed on a way to describe or to tag their respective data, and I will tell you that everybody had their own standards or their own data at that time. Once that was accomplished, the community of interest used the Department's capabilities of the Net-Centric enterprise service program to actually enable the sharing of timely and critical information among the different entities to better secure and protect our coast, our ports and our waterways. This work is still in progress, and the community of interest will span significantly.

To accomplish these kinds of successes, the Department is moving away from a grand design system approach as the basis for its information environment and instead is adopting a service-oriented architecture concept that is key to transforming to a Net-Centric operation. This will significantly improve information sharing between authorized users on the Net. The service-oriented architecture, or "SOA" as we call it, supports an information environment built on loosely coupled, reusable and standard-based services. It promotes data interoperability rather than application interoperability. SOA ensures providers can reuse existing pieces of application and data rather than recreating them every time a new player or an application is introduced. Moreover, it delivers new capabilities and changes quickly to the community of interest. It allows the Department to separate data from the applications for sharing information within and across the global information grid for Net-Centric operations.

The second big challenge I face is information assurance (IA), which was mentioned earlier, protecting the data and defending the network. The importance of IA in protecting information and infrastructures simply cannot be overemphasized in today's threat environment. We have many major initiatives for improving the protection of our information and the infrastructures in the global environment as well as in preparing for future threats.

In order to depend on the Global Information Grid (GIG) as the transformational weapons system that it has become, we must be confident that the network will be available, and we must trust the integrity of the data that is handled by the network. To this end, we continue to follow the tenets of the Department of Defense information assurance strategic plan that emphasizes enterprise-wide systems engineering for integrating the complex IA solutions. By doing so, the Department ensures IA is implemented and managed across the enterprise in a standardized manner.

The Department is moving to managing investments by portfolio. The Department established four capability portfolio management pilots to implement this concept with the objective of ensuring that programs supporting the same capability portfolios are synchronized, that they are interoperable and that duplication is eliminated, ultimately, maximizing the effectiveness of our capabilities. This process is allowing the Department to shift to an output focus model that measures progress by the outcomes. The process offers the ability to look at the whole rather than to struggle to determine if we should be connected between the pieces or the piece parts,

one of the four pilots in this joint network operation capabilities area I am responsible for.

While the Department is moving to the portfolio management approach for managing its investments, it continues to aggressively transform its acquisition processes. Every aspect of how we do business is being assessed and streamlined to deliver improved capabilities with the focus on upfront investment decisions and to ensure that the requirements are defined in terms of effect-based outcomes and that the resources are mapped according to the joint capabilities area. In other words, we are synchronizing the acquisition, the requirements and the resources to ensure successful delivery of IT products and services.

We continue to address ways to improve IT acquisition management and procurement processes. These initiatives are aimed at improving results, saving time and saving money while delivering the capabilities, IT services and other products our customers need on a timely basis.

People are our most important asset and critical to implementing the Net-Centric vision and our goals. We have a close partnership with the Information Resources Management College at the National Defense University to develop graduate-level courses and programs to meet the current, emerging IT management skills needed by the military and the civil workforce within the Department of Defense.

Additionally, the Department has a major initiative to recruit talented IA, or information assurance, personnel under the IA scholarship program, which has been very successful to date. Last year, we awarded 23 new IA scholarships to university students and provided grants to universities and colleges to improve their IA research and coursework. We currently have 75 national centers of academic excellence in the information assurance education located in 31 States and the District of Columbia. This is a real success story.

By now, it should be evident that information and information technology are critical resources in every aspect of the Department's operation. The Net-Centric operation's transformation will enable the Department to become more effective and more efficient. This means timely situation awareness, information that will allow for superior decisions by our senior leaders as well as the warfighters. The Department will continue to emphasize the DOD strategy implementation for information and data sharing across numerous domains, enhance the information protection and improve network defense security. We will continue to transform the acquisition process to put the best IT capabilities in the hands of our soldiers, sailors, airmen, and Marines in a timely manner.

Mr. Chairman and members of the subcommittee, I thank you again for this opportunity to speak to you today. We greatly appreciate the support you have given us, and I look forward to our continued collaboration. I will be happy to answer any questions that you may have about the Department's IT initiatives.

Thank you.

[The prepared statement of Secretary Grimes can be found in the Appendix on page 31.]

Mr. SMITH. Thank you very much.

General Croom.

STATEMENT OF LT. GEN. CHARLES CROOM, USAF, DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA)

General CROOM. Good afternoon, Mr. Chairman, Congressman Thornberry, members of the subcommittee.

My name is Charlie Croom. I am the Director of the Defense Information Systems Agency (DISA). I am also the Commander of something called the Joint Task Force for Global NetOps (JTF-GNO). Thank you for the invite to be here, and I am pleased to be here. I have provided you my written testimony for the record. What I would like to do, sir, with your permission is to address briefly some slides I have provided you. The package looks like this.

Mr. Chairman, if I may direct your attention to the second page, which is entitled, Interlocked Missions. As the Director of DISA, I am responsible for engineering and acquiring and sustaining the global information grid, and as such, I report to Mr. Grimes as my direct supervisor. I have another hat as the commander of the Joint Task Force for Global Net Operations, and in that hat, I direct the operations and defense of the network, and I report directly to General Cartwright, the Commander of Strategic Command.

I mention both of these because these are very synergistic-type roles and jobs where, in one, I am responsible for putting in place this global information grid, and in the other, I am there to operate and defend it, and I think the synergy works very well in terms of an organizational structure. I would add my experience is IT is a team sport, and on this slide are the rest of the teammates. The Joint Staff, the National Security Agency (NSA), the rest of the Office of the Secretary of Defense (OSD), and the combatant commanders are services which I have reporting to me under the Joint Task Force's three-star equivalents from each of the services to operate and defend the network, law enforcement and Homeland Security. So the network ties and is certainly global to everyone.

If we could go to page three, I will try to give you an understanding of the magnitude of this global information grid. We support 31 agencies, 9 combatant commanders, 5 services. We support over 3,500 posts, camps and stations. We have 120,000 lead circuits, 5 million users—the immensity of this is huge—both unclassified and classified networks, as Mr. Grimes described. The unclassified network then is tied to this Internet, and the Internet is both a blessing and a curse, one because you can pull information but, two, because it allows the vulnerabilities to leak to our networks.

If I may refer to slide four, please, Global Presence. To conduct this mission both on DISA and the JTF-GNO, we have a global presence, and I just wanted you to see that we extend across the globe, and the purpose of this is basically to sit at the side of the operators. They are the ones who use the networks to move information, and it is important for us to sit with those operators to ensure their needs are met.

The next slide, please; slide five, Special Missions. In addition to the operation of this Global Net and the implementation, we do

have a number of special missions—providing communications to the President. The White House Communications Agency reports to me. Providing support to the National Military Command Center and the chairmen, 300 folks support that Joint Staff Support Center, fusing information for their needs for daily crises. The Defense Spectrum Organization, not only meeting the needs of strategic planning and architecture for spectrum but also major databases that support the warfighter on the tactical field. The Defense Information Technology Contracting Agency located in St. Louis does over $3.5 billion worth of contracting for information technology. And then the only Joint Interoperability Test Center within the Department of Defense, they are to test equipment before we place it on the network to ensure interoperability and security.

The next slide, please. I would like to address now what I think are some of the good news stories about what we are doing within DISA and what we are doing within the Joint Task Force–Global NetOps. First of all, with your support, you provided funding for something we called the Global Information Grid Bandwidth Expansion, almost $800 million, where we bought fiber instead of leasing, and we own the fiber, and now we are turning it on. The results of that simply are that we have doubled the bandwidth on the unclassified network this past year. We have almost doubled the bandwidth on the classified networks, and that is shown on the slide on the left. On the slide on the right, you see the population growth. Although significant, what it tells me is we are now providing more bandwidth per customer, and this is exactly what we want to do and need to do.

The next slide, please. Slide seven addresses our computing. Where the first slide addressed the transport layer, this slide now is addressing the computing layer, and I think this is a great news story as well. At the top left, you see that we are providing mainframe computing at less sites. Our workload is increasing by 300 percent. At the top right, you see our personnel decreasing by 85 percent. At the bottom left, you see our costs are being driven down every single year as we provide that 300-percent workload, and the best news story of all is, while we are doing this more work with less people with reduced costs, we are maintaining best in class as measured by Gartner Surveys. If we could only do this for all of our work.

The next slide, please. It refers to our commercial satellite services and is, I think, another good news story for the Department of Defense. What you see in blue is what we pay, what the government pays for an equivalent transponder on a commercial satellite. If I can refer you to 2005, you will see we paid $1.1 million for a commercial transponder. The market average is shown in red, $1.5 million. So we in the government are buying a transponder for 25-percent below market average. We are doing that and also improving our processes. We have taken what was a 79-day requirements process and have driven that down to 21 days with a 4-hour emergency response, and as we did the last customer satisfaction survey, we increased our customer satisfaction from a 3.9 to a 4.5 out of a 5 point scale. So, once again, we see costs being driven down. We see our timelines being reduced, and we see our customer satisfaction increasing.

The next slide, please, slide nine. Slide nine really asks you to shift now for second and talk about information assurance and securing the network. These three points are just simply what we do, what we focus on, in trying to secure our network. First is to certainly identify the standards, strong governance, strong configuration management on the equipment and the network, itself, and we have plenty of automated tools that we are bringing on line to do that. The second area is layered defense. We have always had a layered defense, but we are improving the tools from the layer of where we touched the Internet to back to where the user sits. Finally, the identity management, and identity management is simply, do we know who is really using the network? And you might have been aware that this military ID card has a common access card (CAC) personnel key identifier on it, and now, before a DOD member can use his computer on the unclassified network, he has to insert this in his computer where he is now identified. So we have done away with passwords. He now has a physical token plus a pin number. This has, in our estimates, reduced intrusions by at least 46 percent alone. We are at 92-percent implementation across the Department of Defense. Over 10 million CAC card users are issued; 3.6 million are active right now.

If I may, the next slide, please. So how are we doing? Slide 10 tries to address that. You can see the top left. First of all, let me say, this is talking about the unclassified network. To my knowledge, on the classified network, we have not had an intrusion, primarily because it is disconnected from the Internet. It is a standalone, private network. Now, you do not know what you do not know, but to my knowledge, we have not had an intrusion on the classified network, so I am going to be talking just about the unclassified network right now. Now, that does not mean it is less important. Warfighters use the unclassified network. The Defense Logistics Agency orders all parts and supplies across the network, so you do not want toilet paper ordered instead of bullets. You do not want people messing with your network. Transportation command uses this as they move cargo, passengers, ships, as they deal with FedEx and other suppliers, so the unclassified network is extremely important, and we must have it for the warfighters.

The top left shows that the number of attempted intrusions has significantly increased over the last three years.

The top right of this slide shows that, although the attempted intrusions have increased and, I might add, the sophistication of the intrusions has increased, we have been able to start reducing the number of successful attacks on our network, and the bottom left shows that those attacks basically are 2 per 100. That is still too many, but the trends are right, and we are starting now to put equipment in place that will automatically scan and remediate networks, and we are getting much better at this, and we are making it machine to machine. So I think, in my view, we are pushing down on the right train.

If I can now direct your attention to the next slide, slide 11. It is not numbered, but it is called, Acquisition—It's All About Speed. We are now going to shift from the vulnerabilities of our networks to acquisition because I think you wanted us to address that.

My personal belief is that you cannot acquire information technology like we do ships, tanks and airplanes. A 6-year cycle, a 7-year cycle is far too long when technology is coming out at a minimum of every 18 months. I am stating the obvious.

Mr. SMITH. We need to work on the ships, tanks and airplanes acquisition piece, too, as I am sure you well know, but you are right. We need to do better on that, but we certainly cannot have the same principle.

General CROOM. I believe that we can approach speed and stay within the acquisition rules that exist today and the laws today. We just need to modify our processes. So I have tried to list some things that we can talk about in great depth but that I will try to cover very quickly.

First of all, ABCs. Adopt if it exists; Buy commercial, B; C, Create only as a last resort. Too often, we are going into an acquisition process where the acquisition process has already been completed by another—Army, Navy, Air Force—and we refuse to adopt it. We refuse to adopt it because it did not meet our 100-percent requirement, and so I would suggest, do not settle for the 100-percent requirement. Drop it down to an 80-percent. Adopt an acquisition that is ongoing and fall in on it, and we have a number of examples of where we have done that.

Think big, build small, scale fast. It is not a new concept, but the trouble is sometimes in our zeal to do right, we cannot limit what we do, and so it becomes super huge, be it Navy Marine Corps Intranet (NMCI), be it in any number of other instances. So you have got to be able to—in my mind, it is okay to think big, but when you are doing an acquisition, you have got to chop it in chunks so you can deliver it fast, and if you make a mistake, you can afford to make a mistake.

Paralleling acquisition processes. Today, it is a long serial process. It starts on a large program, 18 to 24 months just to define the requirement, 18 to 24 months. Google takes an idea and, in 2 weeks, has it in a lab and, in 3 months, has a prototype and on the network, so we spend 18 to 24 months and 500 pages to prescriptively and descriptively describe the requirement. We could reduce that just by reducing the number of pages, in my view.

Acquisition processes. It then takes us three years to build it. It takes us six to nine months to test it, three months to certify it for security. The way they do it in industry is, when you are building software, they build it, and they have the operator sitting there with you, with the developer. They bring the tester in. They bring the certifier in, and you do it in small chunks and in parallel pieces, and you do not do it in a serial process. It does not break any acquisition rules.

Tailored acquisition approaches. Sometimes you do not have to buy hardware or software. Sometimes you can seek a service, and so we are trying to do that at DISA. Instead of putting hardware on our four left mainframe computer floors, we went and bought a service, so now it is like a utility. So, if I want computer storage or computer capacity, I turn it on like tap water. I do not have to have hardware sitting on my floor.

I have already talked about the requirements process.

Sir, I would like to then close on the last slide just by saying I am fairly optimistic. What I am saying is being echoed across all of my teammates. I thank the organization we have. Between the Defense Information Systems Agency and Joint Task Force Global Ops, it is exactly right on.

I would also emphasize that the Defense Information Systems Agency is a combat support agency. We do not build for ourselves. We build for the warfighter, and so, as we take these needs and build the network out, as we bring command and control programs forward, as we support the logistics world, these are programs that support directly to the warfighter, and so it is really important to us to deliver it with speed because I believe information is America's greatest weapons system, and if that information is provided properly to our soldiers and quick enough, we will save lives and protect soldiers.

So that is all I have, sir. It has been a pleasure to talk with you, and I will look forward to the questions.

[The prepared statement of General Croom can be found in the Appendix on page 46.]

Mr. SMITH. Thank you. Thank you very much.

I have a couple of questions. I think it is an outstanding presentation and shows how we have learned and grown in terms of the way we are going to develop our networks, our computer networks, and I think that is extremely encouraging.

Walk me through a little bit on the NMCI piece and sort of what we learned, how we want to do it better, because that was sort of—you know, the question was not really terribly focused when I asked it at the beginning, but a lot of times, we go for the big, huge system that is going to solve all of the problems, and I thought your 80-percent capabilities point was just outstanding because, when you have got so many different pieces and so many different people you want using the system and if you are holding out for that one big one that is going to make everything work, you are complicating it to the point where it cannot be used.

If you can, walk us through a little bit of the lessons. One of the concerns that has been expressed to me by some people who operate on the NMCI, for instance, is all of the tech support has to come from someplace other than locally because it is this big network system, and they do not have the local IT person who can fix their problem. They spend a lot of time, you know, off line, waiting to get in touch with wherever the center is—in San Diego or Virginia Beach or wherever they have to go to sort of get it fixed. So answer that specific piece, and then, more broadly, what have we learned from NMCI, and what are we going to try to do differently as we move forward and put in place some of these networks that you both have talked about?

Secretary GRIMES. Let me start by saying that I have challenged the Navy on this. We have had a couple of meetings with the Assistant Secretary of the Navy for the acquisition responsibility.

What I have found over the past year that I have been in this job, visiting some of the comments that you have just made or that I heard, is that the user was not brought in, as he was mentioning earlier, when they were developing the system, and when the sys-

tem was delivered, they never anticipated the number of applications that were going to have to be run.

For example, I have heard the number that they started out with at Patuxent Naval Base to be approximately 5,000 applications, and before they knew it, the contractor ran into 14,000 or 15,000. The front-end work on doing this effort was not evidently very well-documented. That caused a delay, and of course, then the contractor who was betting on selling what they call "seats" was not able to deliver seats where he was generating his revenue, and of course, you know what happens if you are in a company like that. They are looking for revenue.

So I would say the largest problem that I have detected—I have been out in Hawaii where they really have had the heartburn—is that initially 10 years ago—or I guess it is 6 years ago now—the operator or the users were not incorporated, and the acquisition community decided what they wanted and delivered something that was not very efficient, and in the meantime, you are in a contract status, and every time you cause a change, you have got a very large bill, and we know during the Timor and during a couple of other major events out in the South Pacific that, when they had to reconfigure the system on the weekends to support Admiral Fargo and then later Admiral Fallon, who they wanted to head the dynamics of the system, it changed. They got a very large bill, which is not the norm in the system.

So I think part of it is probably the way we stated the requirements that the government did initially. The acquisition strategy that was set forth, which is why we are focusing right now with Secretary Etter, is the acquisition strategy, and I have an expert who is working very closely with them.

So I do not know if you wanted to answer.

General CROOM. Well, it is very easy to Monday-morning quarterback.

Mr. SMITH. I would not look at it that way. I would just think of it as sort of lessons learned.

General CROOM. Okay. First of all, I would say it is a very noble goal, and I had nothing to do with the acquisition. My personal view is that they were trying to catch up, if I may, with the other services who I believe were far ahead in terms of their network technology, and so I give them credit for trying to put money down and solve a problem.

The first issue I think Mr. Grimes had exactly right was that they did not know exactly how big the problem was. See, these networks were not installed under a program. When I was a lieutenant and a captain, we were with a bunch of good sergeants, and we started taking and putting computers on desktops, and the next thing you know, we were running and cutting holes in floors and walls and connecting these things, and so they were put up by a bunch of hobbyists because, at the time, none of the services had programs to do this, and it stretched out as a hobby—no configuration management and no security—and so this network of 15,000 different networks that are in place today were all built by different people under different circumstances under different methods.

Mr. SMITH. So each went down and sort of pulled that big mess together.

General CROOM. Right. So they did not really understand how nonhomogeneous this thing was, and so then when they got there, they also found, as Mr. Grimes mentioned, thousands of unique, independent software running on this network that somehow they had to interface. So those two problems alone were very difficult.

Now, if we were to do it today, I would suggest chopping that problem up into smaller chunks. Prototype so that you can learn what you are doing on that first chunk, and then take that knowledge before you deliver the second chunk and the third chunk and the fourth chunk instead of trying to tackle it all in one gulp.

The only other disagreement if I could—and I am speaking from DISA, from the Air Force, when I had to write a report to Congress on why we were not doing an NMCI-like approach. The Air Force at the time believed that it was very important in terms of having the right mix of people operating and sustaining the network, and the Air Force's philosophy at the time was one-third military, one-third civilian, one-third government contractor. There was great synergy there. One, we felt the network, because they were a warfighting network, was important in order to have some sustainment of talent within our own Air Force, but usually, the young airmen could not keep up to the civilians who had been working there for years and who had been in place for years, and the contractors, what they do is they bring in new technology.

So, between the one-third, one-third, one-third, we have the high energy of a young sergeant who is learning the business. We have the sustainment capability of the civilian who has been on the job for a long time in the ops center, and we bring in a contractor who can bring new technology, and they learn from each other. So I think that still applies. Unfortunately, a lot of times, either personnel cuts or budget cuts drive us to one solution or the other, but I would say I stick to my rules, and I will think big, but I will build small and where you have success scale rapidly.

Secretary GRIMES. I would like to follow up just on two points. One is that it has not addressed the interface with the classified networks which the Navy has to operate and which goes back to our Net-Centric operation, so that was another thing that took a lot of time and, in fact, has not been totally fixed.

Second, we are working closely with them on their acquisition strategy to do part of the approach and breaking the program down somewhat where it would not be one contractor turned key, and so that acquisition strategy has been working great.

Mr. SMITH. Thank you very much.

Mr. Thornberry.

Mr. THORNBERRY. Secretary Grimes, you have responsibility to set standards for IT, which is purchased by the Department of Defense, and yet, you do not have control of the money that is used to buy the stuff.

Talk to me a little bit about the tools you have to ensure that services and others comply with the policy standards that you have set, whether that is enough and how that works.

Secretary GRIMES. Well, I do have quite a bit of control, oversight of the money, although I do wrap up the total budget of the De-

partment, but there are a couple ways that I like to enforce where we are going. The standards we use—by the way, they are mostly commercial standards as you well know—are the—I had in my mind the two or three things that I was going to say to you. I will have to back up.

General CROOM. Well, while you are thinking about that, I would add that he also has me as a tool.

Secretary GRIMES. Oh, I know. Here is what I want to say.

I am also the Milestone Decision Authority (MDA), the acquisition authority, which they have to come through me, the service for all of their major acquisitions. I was trying to get the flow.

So I have oversight but also the MDA, or the Milestone Decision Authority, which is delegated to me for IT from our Acquisition, Technology and Logistics (AT&L), or Secretary Krieg. So I do that.

Third, there is also some oversight that sometimes gets in our way, and that is the Inspector General (IG). They have a responsibility. On the front end, they have gotten more active in recent times. So that is another way of finding out if someone is off.

Last, I mentioned to you earlier in my remarks "portfolio management." As we move into portfolio management, we are going to have all of those folks who have got to come to us under our portfolio now and look at trades, and that also, if you will, enforces some of the things in looking at duplications and synchronization, and we are in a position now with the new process that has come out of QDR called the Deputies Advisory Working Group, the DAWG—I do not know if you have heard of this or not. It is very effective and I sit there. So those checks and balances, I believe, today give us quite a bit of say. Also, I have a CIO counsel through the Department of Defense, and we have a pretty effective operation or coordination and collaboration in that.

So, in that regard, I believe today we have that pretty well under control. That was one of my questions, actually, in my original confirmation hearings was the budget process, and I was not aware—I had not worked on that side, and I had been in the Department before. I was more on the command, control, and communications (C3) side, which is different than the IT side, but I believe the things that have happened in the last year give me—I submit the budget, the IT budget, to Office of Management and Budget (OMB). It is my shop that does that. So we have a very good picture of what is happening in it.

Mr. THORNBERRY. Okay. Thank you.

Mr. SMITH. Ms. Castor.

Ms. CASTOR. Thank you, Mr. Chairman.

Thank you, gentlemen, very much for your presentations.

I was interested in the positive trend on vulnerability reduction. Can you share with us what you believe the new vulnerabilities are and the sources of potential attacks and then what you are anticipating the future holds?

General CROOM. I certainly can share in a general way, and the sources of attack I will kind of have to defer to, maybe, a classified session, but the sources in general—the first way an intruder gets in—by the way, let me start off by saying we have seen a significant trend move from the hacker to the criminal, who is still very active by the way because they are making money on these intru-

sions, not off the government so much but off of the commercial world.

We are seeing some more nation-state actors come on, so they are a little bit more professional. I will just leave it at that.

The first way they get in is through passwords. It was the number one way. It was the front door, and they got in quite easily. The name of your dog just was not a good password. They can break that very quickly. So that is why the Common Access Card (CAC). Like I said, as soon as we implemented this, we saw a significant change in the way the intruders were acting. In fact, when we implemented this, what we saw was what we call phishing—socially engineered e-mails trying to get your passwords. We saw a significant increase in that. So they are very reactive. We can sometimes see their responses within hours.

Ms. CASTOR. How are you able to monitor that? Is it something in the system?

General CROOM. I would refer that question as well, if I could, to a classified system, but you know, we have capabilities, automated capabilities, that look at intrusion activity just as we monitor the network traffic across the network.

The second method for getting in was software vulnerabilities. Software vulnerabilities come in all software. Microsoft is a good example. We look at about 300 vulnerabilities a month. We selectively identify a number of those and pull them down and issue patches across the network. We have significantly improved our ability to do that, and when we started this about 3 years ago, we issued 18 patches over the entire year. In January of 2007, we issued 19 just for January. So our ability to issue patches across the network and our efficiency in patching has significantly increased.

The third method then is—you hear about botnets. This is where a computer can control many computers, and then criminals actually sell these thousands of computers that they control for other means, but the way they control your computer is because something in your computer allowed them to control it. You did not have a good configuration. So we have set standards to the configuration of that computer. We have a gold standard, and we lock that computer down, and we significantly reduce the ability for them to come in and control. In fact, in the numbers we have, we have seen a 110-percent increase on the Internet for these botnets, these controlled networks. Over the last year, we decreased 80 percent on our dot-mil network, on our military network. So configuration standards are extremely important, and we are now getting the tools in place to lock those machines down and automatically check them, and you know, when you have five million users on your network, you do not want to be doing this manually. So we need your support as we go and identify the automation tools to be able to scan the networks and lock those networks down.

Mr. SMITH. Mrs. Drake.

Mrs. DRAKE. Thank you, Mr. Chairman.

Thank you both for being here.

I would like to ask you—because I have heard two things on this. I have heard there have been concerns regarding our IED jammers and our communication, that our troops in the field would either

be doing one or the other, and certainly, they need to be able to do both. Then I have read that the Navy has helped the Army, and the Army can now operate these jammers so that they can also communicate.

So I wondered which it is, and if it is still a problem, what can this committee do to help in that endeavor so that we are not putting our troops in theater in that position where they are picking one or the other?

Secretary GRIMES. Well, I was in the theater a year ago at this time, and that was one of two major issues. One was sharing information across various domains, but the other one was spectrum, and this is a spectrum issue, a radio frequency issue, and at that time, it was pretty severe. We were interfering with our own self, if you will, and the IED issue was not as pervasive a year ago as it is today.

Now, with that said, the Navy loaned the Army in this case electronic warfare officers to go out to assist because of a couple things. The Navy electronic warfare aircraft are used to hopefully, what they call, "burn," "explode" the IEDs before the time, you know, they go out. That interferes from that airplane. So, today, they deconflict before the mission to allow the Army or the Marines to know that this mission is about to take place at this time before they go out and do an IED mission. So it is a very complex operation, and it depends on where you are, too, in the location and the type of jamming that you are going to do of the IEDs or set them off. There are a number of things that they use. By the way, the enemy just changes as fast as we change to the newer technology. Some of it is just quite scary.

So it is not either way. It is an operational—and it goes back again to information sharing. In fact, when I was over there, one of the problems they were having in Afghanistan is that the information was not getting to the units that were out looking for IEDs if someone else had identified an area earlier, and I will tell you they had lost four Army engineers, at the time I was there, looking for IEDs, and they felt that the information was not being shared, but I think a lot of that has been resolved. The other part of that was the communication shared, the type of radios that are with the IED force at that time, including some satellite capabilities, direct.

Mrs. DRAKE. So it sounds like there is good progress, and if there were something you would need this committee to do, you would let us know.

Secretary GRIMES. Yes. I know that General Meeks is doing a great job in his task force. I have the Spectrum business for the Department of Defense. We work very closely with them, and we also have a major program. In fact, General Croom is the office that manages the Spectrum for us—I am the policy guy—and we are working very closely with them.

Mrs. DRAKE. I just have one last question, General, and I am glad to hear that you are using off the shelf, that you are talking about the 80 percent, because I have had it brought to my attention where people think we are purchasing programs or going out into the private sector in contracts and having things created for us that we are not able to continue using, that you might have it for you, but possibly Homeland Security could use the same thing.

Is there a crossover so we are not recreating the same thing and spending taxpayer dollars on the same technology that might have been created for you or is there some way to make that happen? I know there is an intellectual property right, too, if you create something, but if we buy it, as taxpayers, for Department of Defense, is that available now for other government agencies?

General CROOM. Well, first of all, I think this is an area ripe for improvement in terms of sharing although it has been on our list to do for many, many years. It is hard to know what is out there. It is a four-year share, number one. And two, sometimes a contracting vehicle limits your sharing. The boundaries of the contract will say sometimes you are procuring this for the Department of Defense so you cannot share it with Homeland Security. Sometimes that contract will say you are buying it for the Air Force, so you cannot even share it with the Army or Navy. It is kind of interesting the way the acquisition rules are and the way they are applied, but you have to look at the rules of the contract in which the product or the service was acquired and whether that contract permits folks outside the boundary that was originally established to use it.

There are many things out there that can be adopted, and like I said, the problem with adoption is you have to fall off your requirement. That is the culture that has to be changed. Once the culture changes, you can, you know, make other things happen.

Mr. SMITH. Is that simply a matter of the culture or are there regs written that make it more difficult if you come back and say, "Hey, gosh. This is a great thing out here, but it is only 80 percent of my requirements"?

General CROOM. Yes, there are some regs. Obviously, when you write a requirements document, sitting on top of that requirements document is key performance parameters called KPPs under the joint staff. Those key performance requirements specify what you have to deliver to.

Mr. SMITH. Is there something we can do in committee here that could give you greater flexibility on that piece?

Secretary GRIMES. Well, I would like to interject something here. You have got to watch when you talk software as you get closer to a weapons system where it may be designed for that, and on the other end where it is more of a common user—Windows or Microsoft or something like that—we do have a program that has been a real success story, and OMB is looking to adopt it, and it is where we think we have saved a void, I should say, of about $2.5 billion since 1999. It is the sharing of contracts and buying software. The Air Force, in particular, has been a big user of that. So there is unique software. Then there is the common off the shelf, and I think that we have a pretty good program to say it has been around, and we would be glad to share that with you, but I can tell you, the closer you get to a weapons system, the embedded IT, it is much different.

Mr. SMITH. But I mean that is very specialized. That is not——

Secretary GRIMES. Correct.

Mr. SMITH. Let me make it clear. When I say, you know, you only meet 80 percent of your specs, I mean, if it is a weapons system, it is like, you know, we meet 80 percent of our specs, you

know, and this will get to its target. It just does not blow up. I mean, I understand that there is a point at which 100 percent is absolutely required, but based, you know, on General Croom's comments about—if you are looking at, you know, going from—that the Army has got a system, you know, set up that may not be commercial but may be internal but it fits 80 percent, you know, of Air Force specs, that is what I was asking, and I think you were going to try to take a stab at——

General CROOM. I was trying to think of something before I put my foot in my mouth.

Mr. SMITH. That is all right. We do not have to do that over here. We are blahhhh. You are more cautious.

General CROOM. Sometimes in our zeal to get it exactly right, we would put our requirements in such specificity that it becomes technical requirements. So they are not broad statements of capabilities. They become technical—milliseconds of delay, a number of screen refreshes. How many objects go on a common operational picture? It is in the tens of thousands. So then, all of a sudden, you are stuck to a specific number that might have been good the day it was developed but is not going to be good a year and a half from now or two years from now or whenever when you are delivering this or it ties the hands.

So I think that this is not a legislative problem. I think this is something that has to be worked within the DOD as we learn to improve our processes. We need to specify the criteria on which we require things in broader statements and not specific statements to allow a little bit more flexibility in what we are delivering to.

Mr. SMITH. What would the flexibility be? Let us say you had a situation like the one you just described, and they write the regs that they want, and you take a look at it and go, "Well, wait a second. We have got this great product out here that does not meet this one, but that one should not be a requirement." What is the flexibility at that point to go, "Hey, can you change these"?

General CROOM. Well, it is a long process.

You know, General Kadish wrote a report. He was the missile defense lead. Then after he left office, he wrote a report which I think is available to you all, but one of the things he talked about was sometimes when you are developing something new and you have gotten—the last 20 percent of the requirements is always the hardest to build to—okay?—but sometimes the 80 percent that was delivered is 5 times better than what you have in the field, but you are not able to pass the wickets and deliver it to the field because you have not met the final criteria, the 20 percent left. So General Kadish was recommending, you know, it ought not to be the acquisition czar that makes the decision on whether the capability can be delivered in the field. It ought to be the operator. The operator ought to say, "You know, I know it is only 80 percent of what we originally thought we could deliver, but it happens to be 5 times better than what I have, so I am ready to have it delivered," and so I think those types of things are being discussed within the Department.

Mrs. DRAKE. And I am wondering, Mr. Chairman, how we can keep trying to get our hands around this issue? Because yours is a little different than what my concern was, which is that the tax-

payers are out there always recreating the same thing and, like you said, not even having a way to know that this has been created for Homeland Security, and now you are looking at some system to watch the border in Afghanistan, and do we have it over here? And they do not seem to be playing well together.

Mr. SMITH. Right. Well, I think it is not so much they are not playing well together as it is they are operating their own stovepipes. There is not a conflict. Well, a good example is—take that question out.

I mean, when you are looking for a system, do you think and go, "Okay. This seems like a similar thing to something that Homeland Security would be doing. Let us take a look and see what they have got"? Do you do that? Is Mrs. Drake right? Are there then sort of, you know, territorial blocks at that point?

General CROOM. Yes, I think we have to do that to be good stewards of the taxpayers' dollars. It is very difficult to know, though. I mean, these are big, big, large organizations, and to do that search and to do it reasonably is a very difficult task, and then you have the cultural differences, and again, you know, it is always after they describe it. "Well, that apple is not what I really wanted. I wanted the orange." So it was not close enough. I mean, I will give you an example.

DISA had to develop a portal. I just came from the Air Force to DISA. The Air Force was developing a portal. DISA is developing a portal. The Army has a portal. I went to my folks at DISA and said, "Well, why don't we use the Army portal?"

"Well, their portal is not as good as ours. It is not architecturally developed as well. It is not engineered as well."

So I asked, "Well, how many users are on the Army portal?"

"One point eight million users."

"How many users are on the DISA portal?"

"Forty thousand."

"Okay. So what is the decision?" I said, "Move over. Let us adopt the Army portal. Let us make that a joint portal. We will spiral that out."

So that is what we collectively agreed to do. Across the Army, Navy and Air Force, we adopted the Army portal, not because it was the best solution. It just happened to be the biggest one, and we could then move them forward in a future spiral to improve their architecture. So that is the type of thing that needs to be done, but it is very difficult to do for a lot of reasons—the way the money is, the years you get the money, how you share the money across services, the technologies, you know, the culture. It is very difficult.

Mrs. DRAKE. Thank you very much.

Thank you, Mr. Chairman.

Mr. SMITH. Thank you.

Mr. Conaway.

Mr. CONAWAY. Thank you, Mr. Chairman.

In my business background and even in our own office, we typically replaced all the hardware on an average of every three years. Right or wrong, that has generally been the model.

Do you have a similar goal, and if so, where are you in terms of being able to keep up what you think is the most prudent replacement just on the hardware side?

General CROOM. The services basically have a similar goal. Although, I think it is expanding out because we did that early on as the desktop computer was significantly growing in capabilities. Now that desktop computer is far superior to the capabilities we almost need, so I think you see that trend slowing down and starting to stretch out. That is not a DOD mandate. The services buy their own equipment. The Army, Navy and Air Force buy their own equipment, but basically, they have a three- to five-year replacement rule on average.

Mr. CONAWAY. Everybody buys separately. How do you collectively continue to make those decisions? It seems that everybody is buying. How does that work.

General CROOM. Actually, the services do have, group their requirements together and buy large buys and actually drive the price down very, very well, well below the market average price for end items on desktops. I think they are very, very good at that.

Mr. CONAWAY. Is your group responsible for making sure that all computers have a licensed version of Microsoft XP, whatever, those kind of reviews and audits to make sure that we are at least obeying all the intellectual property laws across all of our networks? Do you do it? Where is that done?

General CROOM. That is done at the individual service level.

Mr. CONAWAY. Thanks, Mr. Chairman.

Mr. SMITH. I want to follow up on the acquisition piece, putting aside for the moment the requirement discussion. That was helpful. What about in terms of other transactional authority and the ability of your contractor to go around the regs and just see something on the shelf and say that is what we need and not go through the normal procurement process, so when, I guess it is the defense information technology contracting organization that is responsible for this, what is their flexibility? Well, I have asked the question.

General CROOM. Sir for large buys, you just can't go around the rules.

Mr. SMITH. How large?

General CROOM. There are dollar thresholds. I don't know them off the bat, but usually when we do buys like this, it is for the Department of Defense. And I will take an example, we just bought a collaboration tool it was IBM Sametime. And we had to—that is an off-the-shelf piece of technology. We had to write a Request for Quotation (RFQ), compete that. That takes months. Then that is awarded. And then you stand by for a protest.

Mr. SMITH. Right.

General CROOM. And this takes a couple of months.

Mr. SMITH. Is there any way, and this is—it is a cottage industry, but it is a little bit more than that and this is all across the DOD you mentioned the protests and obviously there are private contractors out there and we are going this on every conceivable level. The one that leaps to my mind is the tanker issue.

And obviously, there is some nasty little aspects of that that are outside the norm. But forgetting that for the moment and just sort of focusing on hey, you got this big thing, the military is going to

buy it. There is several private contractors that want a piece of it. You have to go through the process and they are going to fight like cats and dogs over it. And it gets appealed. And I imagine the same thing happens with IT you can imagine various companies out there that provide a product. They don't win it. And they come back and call us. And we fight this out.

And my bias about all this is a little opposite of what is going on here right now. My bias is to actually give greater power to folks like you and those below you to make those decisions.

My second bias is to then fire them if they don't do it well instead of tying their hands and making it impossible for anybody to do it well. But we have all these contractor issues that are floating around out there.

Is there any—if you could sort of cut through that and say here are two or three things that we can tighten up to greater empower your people to make these decisions without having to go through that process without facing those appeals what are some ideas you can throw out there?

General CROOM. Well, first of all, I like your approach. Give me the authority and fire me if I screw up.

Okay, today, the rules are such that you almost could do nothing on a three-year tour and be well within all the laws and acquisitions.

Mr. SMITH. And be promoted.

General CROOM. But I would have to suggest I go back to my ABCs. I avoid all this acquisition problem, all the release of the RFQ, the bids, the proposal reviews, the protests, if I can adopt something that has already gone through that process. That is why I love adoption if I can find something that meets the 80 percent rule, adopt it and spiral it all out. The only thing I have to worry about is if I am adopting something, does that contract allow the flexibility to meet the participants I need to have? Does it allow the flexibility? I don't know what else to say about it.

Secretary GRIMES. I would like to interject something here too. The services are allowed to buy a lot of stuff but we look at everything from an enterprise. And General Croom's focus is primarily on those that are going to operate in a joint environment. And so we want to make sure what the services are out there buying for their own use, will end operate, will operate within our environment.

He has a test capability that certifies so there is two aspects of it, what you ask, one, that is he talked about the acquisitions front end which is laborious. But the second side of that, we do have to bring, in order for someone to put their capabilities on his network, goes out to Fort Huachuca and goes through this test phase it is like the underwriter code or mark.

So there is a lot of dynamics in that area to ensure—and I don't want to call them, we have standards in the sense of the standards you would normally harden asset standards, but there are standards that you have to meet to operate to the network and make sure it doesn't impact the network when it gets on there. So that is a very good program that has been around probably 15 years. So anybody in the joint arena that wants to get on our networks has to go out and get recertified.

General CROOM. So this dilemma you have is, freedom is wonderful but then you have to—you are trying to worry about what are they buying and how does it fit into your enterprise. And does it meet the interoperability and security issues? And so all of a sudden then now you are starting to put requirements—I mean, it builds on itself. It is a balance.

Mr. SMITH. It is, and I don't mean to imply meaning if we just did it the other way we wouldn't have any problems. It is just a matter of striking that balance. And my impression right now that is the balance is too far tilted to the process as opposed to the action.

Secretary GRIMES. I am going to—I won't make any mentions but the service have received a lot of money over the last number of years. And a lot of that money went down to units that normally would not get the amount of money and they go out and buy things at Radio Shack, whether they are emitters that Mrs. Drake was talking about or software. And we have very bright lieutenants and captains out there that will come up with solutions. And when they put that solution on his network, there is two things can happen. It can impact the networks operation, but second, is there a security hole that it may open?

Mr. SMITH. Oh, yes.

Secretary GRIMES. And this is an area that concerns us very much. And his other hat, his Global Net Operations (GNO) hat, hopefully he identifies when someone is on there unauthorized or is doing something they shouldn't be.

Mr. THORNBERRY. Mr. Chairman, it does occur to me with this last conversation that essentially we are trying to do things in the Internet age with an industrial age bureaucracy. And you all probably feel it as much as anybody in IT. And I think what chairman and Mrs. Drake both are saying is, help us look for ways to improve this. It is not just legislation. It is not just regulation. But I see it as kind of a microcosm of how we are going to have to be more flexible and adaptable not only in what we buy but how we react to the world around us.

So if I could ask another couple areas right quick I know that private industry was surprised by the rapid increase in what chips can do and the power requirement that came with that.

In looking at the size of your responsibility across the Department of Defense, and using that as an example, is that something that caught you by surprise? And how do you deal with something that has that many consequences?

General CROOM. Are you talking about computing power? The growth of computer power? Moore's law has been known by all of us for a long time.

Mr. THORNBERRY. I tried that but as I understand it, and I can't get into all of this, but, there has been universal surprise at the increase in power that has been required to run the increasingly productive chips that——

General CROOM. You are talking about utility power?

Mr. SMITH. And also keeping it so the chip doesn't overheat the whole system.

General CROOM. We have been out now, we do many visits to industry, Microsoft, Google, Sun, they actually know when you talk

about the size of their computing rooms, they give you the size in terms of kilowatts consumed, not in square footage. They are physically moving their computing facilities to be right alongside producers of energy like below a dam or whatever, because they don't want to pay for the transport of that energy. So it is a significant cost to industry.

I don't know yet if it is a cost driver for government. And I say this putting my own foot in my mouth, sometimes I believe our personnel costs are our cost driver right now and energy might be second. But for industry they have the personnel factor so low with lights out processing that now we are going after their highest cost driver, which is energy.

Secretary GRIMES. Of course, we have found where some of our super computers are operating that we are having problems of getting power, in fact, shutting down if you will so certain missions can be done 24 hours a day. And that is a real issue. And even where the power company has the capability to give us that—in the near future that is and maybe that is what you are referring to. That occurs to me as a surprise to——

Mr. THORNBERRY. The surprise comes out, but it has enormous ramifications and it even exacerbates what we were talking about the need to be flexible and adaptable. Maybe it is just a big super computing type operations that affected and maybe the more, you know, the lesser levels are not so much.

Can I change the subject right quick? Secretary Grimes, do you get into—I notice in your statement you talk about defense business transformation efforts. Does it come under your responsibility to find us a way some day that we can track money through the Department of Defense? Where one system talks to another and that it can even pass an audit?

Secretary GRIMES. Well, you mentioned business transformation. As you know, it was established before my watch, the Business Transformation Agency to address, I think it was mandated by the Congress, for the business systems. Two things, I participate on that board with the deputy secretary and all of the others, and, in fact, it is co-chaired by the Deputy Secretary and Secretary Krieg to run the business systems and that whole process.

Second, I have a role, because of my title 40, Clinger-Cohen, both the budget comes up through me and second, we, through the MDA, my milestone decision authority, that comes through me. So I do have some checks and balances.

Mr. THORNBERRY. It is an excuse I have heard for 13 years now the reason the Department cannot pass an audit is because its IT systems can't work together, so that they can't, one system can't talk to another and so when you try to say, this dollar comes from the taxpayers, and it goes where? And ends up where? You can't answer that question.

Secretary GRIMES. That is a very good point. And that is one of the highlights about that centricity or data strategy of sharing data across the financial systems, which I think you are also probably referring to. And today, hopefully, I believe some of the things we are doing, I mentioned the maritime domain, how we took that in nine months and the interagency process, well, we are now working

that internally also for sharing information between those business systems if you will.

Mr. THORNBERRY. So when are we going to fix that?

Secretary GRIMES. You mentioned 13 years. I am hoping it is not another 13 years, but——

Mr. THORNBERRY. I may not last that long.

Secretary GRIMES. I know I won't.

Mr. THORNBERRY. Mr. Chairman, with your indulgence.

General, once upon a time I was told that something like 90 percent of DOD's IT is dependent upon commercial infrastructure. I don't know if that is exactly right or not but when you talk about defending the networks, the question that I have a hard time understanding is, who is responsible for defending the commercial networks, or the commercial infrastructure upon which our networks depend? I spent some time on the Homeland Security Committee, and I spent some time here and there and around. Who is responsible for that?

General CROOM. I can tell you who I think is responsible. I know it is not the Department of Defense in terms of—my mission is bounded solely by the DOD military network. And the DOD military network is made up of 120,000 leased circuits, commercial satellite communications, and we own some of our own obviously. We work with Mr. Garcia from homeland security, my commander as a joint task force global net ops, we share our operational threat with them, we share our operational status, we share processes, techniques, tactics and procedures. But right now there is, I don't believe, any capability to look across the entire commercial network. You didn't ask capability. You asked who is responsible.

Mr. THORNBERRY. I am trying to start at one place, but yes.

Secretary GRIMES. Could I intercede there? I don't know if you are aware of the President's National Security Telecommunications Advisory Committee that has been around since the early 1980's that was brought into place by the divestiture of AT&T. And it looks at national security emergency preparedness. And today, that function was transferred, actually out from under General Croom to Department of Homeland Security (DHS), it is under Garcia. But the purpose of that was to do exactly what you are talking about, and the awareness with those companies, and, in fact today, I just drove back from Cambridge, Maryland where we had the industry down there, part of the President's Advisory Committee, on how we improve their infrastructure that supports us.

Everything from power, emergency power, to how you recover a 9/11, which they did a very good job by the way, and we have set up this national coordinating center for telecommunications with industry and government in it, which actually supports his GNO mission also, and so some of that is in place, and has been around for quite a while.

It was put in place for the nuclear, the Cold War. Now he has evolved to support the new generation or what we call the next generation networks convergence network. But they are the source. And in his building right today you have government and commercial carriers, the Verizons, AT&Ts setting in that facility, along with others, with other government agencies, that is looking at that network they are dependent upon.

That part is going to be moved, I believe, out of his building over to DHS center very soon which is a concern to some people but that process is—and the President meets with those individuals once a year, next month he meets with them, and when I was on the national security staff, that was one of the things in my portfolio that was quite effective. And they put in place if you will, capabilities into that network on priorities, what is going to be restored, how you get fuel to those critical nodes, owned by the telephone company, that process preplanning has been put in place for a long time.

Some of it also goes back to how you continue to operate in a distressed or disturbed environment, interrupted, disrupted environment, so——

Mr. THORNBERRY. I think it is going to take more than a coordinating committee, and I have some concerns that the authority is not where the capabilities are. But rather than pursue—Mr. Chairman, I have a few other questions kind of in this area that I would like to submit for the record. But I think it is something that probably a lot of us need to continue to investigate. And I yield back.

Mr. SMITH. That is a very helpful line of questioning. I appreciate that. I just have one final quick question off that. In terms of personnel in terms of getting the people who have the technological talent to do the job you need at the DOD, are you able to recruit the people you need? Is there more you need to do?

General CROOM. Yes, sir. I am able to recruit the people but we have a very aggressive recruitment process. Of my 6,600 government employees, I think we have an intern program that starts spotting these folks—technical folks, engineers, computer scientists, while they are still in school and we bring them into DISA and part-time work and we bring them in as a 3-year intern. And we probably of 250 to 300 those folks—120 a year—and it is a 3-year program. So we aggressively go out and recruit and they have some obligation to stay with us.

I will say Mr. Grimes was mentioned in my area to mention one thing we have we will have a problem here shortly as we have been Base Realignment and Closure (BRAC)'ed. We will move out of Washington to Fort Meade to be with our buds at NSA. That move out of Virginia into Maryland I will lose a significant portion of my technical workforce just because they have been in place for a long time and they can get jobs anywhere. And they will not tend to move. And so this will be a significant issue as we work that. Thank you.

Mr. SMITH. I have nothing further. Mr. Conaway, do you have any further?

Mr. CONAWAY. One. This may be too simplistic to embarrass myself. As we buy thousands of laptops and computers every year each one, in my view, is potential vulnerability to user access points to the overall network, both from a Trojan horse if the machine itself has something in it that shouldn't be there, it is configured the right way, are there—and obviously, this is something you know about this, or do you have the right infrastructure in place to watch for those things? Because everybody is buying separately, are there seams in the overall protection that can be exploited?

How do we make sure that we keep them all updated and the right encryption gear on them and all that kind of stuff?

General CROOM. Again, I don't buy desktop computers for the Department of Defense, so I will answer just what we are doing at DISA. And obviously, we don't want to be the next Veterans Affairs (VA) where a laptop is stolen and information then becomes available.

So we have got to encrypt the data that is on the laptop if it is taken away from the facility. But more importantly, again, you can't get into the laptop unless you have your personal identification card and have it inserted into the machine and provide the proper Personal Identification Number (PIN). So that helps secure the information that is on the laptop. Plus we are working methods to secure the data what we call data at rest, data that sits inside your laptop.

In order to connect back into the network to do your work or retrieve information, again, you can't do that without your physical token plus a PIN number. So we are trying to address just your very good concern.

Mr. CONAWAY. Would there be a Lieutenant General Croom equivalent at each one of the services to make sure that they are doing the same thing?

General CROOM. Absolutely. Absolutely. And in fact, I will repeat under the Joint Task Force Global Net Ops I have an organizational structure to get back to your question. I have authority. Now my authority, first of all, is delegated to me by Strategic Command (STRATCOM). But I have authority to direct actions across the network. If we want to shut ports and protocols, if we want to redirect any actions, if we want to secure something, I have the command authority to do that and I can order the Army, Navy, Air Force, 31 agencies, 9 Combatant Commands (COCOMs) to do it.

I can order patches on the network. I have the authority and we are exercising authority. We ordered the implementation of this cat card, and of course, with authority comes, you have to track it or else you have a weak policy. But we track it and we enforce it.

So the services have that structure below them and they have a three-star in charge of their networks that report to me. So they have a very good structure as well. So it is—we are the military.

Secretary GRIMES. Of interest to you also about sharing information Mrs. Drake, we meet, the Chief Information Officers (CIOs) or the C–4 or whatever you want to call us on meet on a—every month, and compare notes and we let our hair down and do these things he was talking about sharing it. The Army has something that they can adopt to or the Air Force, and it is a lot of synergism taking place in our community because of that and they are all highly technically inclined, I am here to tell you a lot of good things are taking place you don't see on the surface.

Mr. CONAWAY. That is terrific. But are there circumstances where you collectively come to the place you want to implement and you can't, do you have an appropriate way to push that further up so that you do, in fact, get what you want?

Secretary GRIMES. I am the guy I guess where the buck stops in this area. And then, the Deputy Secretary who I work for, and the Secretary who I work for, I usually, and he happens to be in tune

with our technology. We haven't lost any yet to where we have had any issues.

The biggest thing we have right now is the IA, the information assurance area, and how that is done. And of course, NSA provides most of that. We work very closely, he is the organization that implements it. But that is where it is going to get costly, protecting information and protecting the network.

Mr. CONAWAY. Thank you, Mr. Chairman.

Secretary GRIMES. It is a big bill.

Mr. SMITH. Well, thank you, that is all I have. I do believe you gentlemen are doing a very good job. Obviously, there has been a rapid pace of change, but I think the Pentagon, in the last four or five years, in particular, has stepped up and tried to figure out how to make the best of that change, meet the challenges and take advantage of opportunities, obviously more work to be done. But I am very impressed with the testimony and looking forward to working with you to keep that process moving forward. Thank you for coming today, we are adjourned.

[Whereupon, at 3:30 p.m., the subcommittee was adjourned.]

A P P E N D I X

MARCH 28, 2007

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 28, 2007

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
SUBCOMMITTEE ON TERRORISM,
UNCONVENTIONAL THREATS AND
CAPABILITIES,
HOUSE ARMED SERVICES COMMITTEE

STATEMENT BY

THE HONORABLE
JOHN G. GRIMES
ASSISTANT SECRETARY OF DEFENSE
(NETWORKS AND INFORMATION INTEGRATION)
AND
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL
THREATS AND CAPABILITIES
HOUSE ARMED SERVICES COMMITTEE

ON

DEFENSE INFORMATION TECHNOLOGY

MARCH 28, 2007

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
SUBCOMMITTEE ON TERRORISM,
UNCONVENTIONAL THREATS AND
CAPABILITIES,
HOUSE ARMED SERVICES COMMITTEE

Introduction

Good afternoon Chairman Smith, Congressman Thornberry and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee on Terrorism, Unconventional Threats and Capabilities on the importance of information technology (IT) to the overall missions of the Department of Defense (DoD). I am John Grimes, the Assistant Secretary of Defense for Networks and Information Integration and the Department's Chief Information Officer (CIO). My statement will focus on how the Department is leveraging information and information technology (IT) to rapidly respond to unpredictable, unanticipated and unknown global national security challenges of today and tomorrow.

The 2006 Quadrennial Defense Review (QDR) states that achieving net-centricity is critical to "harnessing the power of information connectivity." As we move forward to support the Department's Transformation and the QDR goals, the focus of net-centric operations and activities is ***to provide a more effective and efficient force***. That "force" includes the warfighter, the intelligence community and the business processes that support and enable the warfighters' success. Regardless of time or place, each different element of the force must be able to say, "I can get the information I need to perform my mission," and our transformation efforts are focused on enabling that.

Net-Centric Operations

The ability to access information, to share the information and collaborate with others is at the heart of net-centric operations. To make this happen, we have established four fundamental goals—to effectively build, populate, operate and protect the information network. To '***build***' and modernize our network, we must ensure that the latest technology and infrastructure is available so that the warfighter can operate in a speed-of-light information world. To effectively ***populate*** our network with critical and timely

information, we must provide the mechanisms by which data can be posted or stored and readily accessed by users. To ***operate our*** enterprise network we must ensure that data is accessible, reliable and available whenever and wherever it is needed, while at the same time ***protecting*** our network against an adversary who is determined to exploit the cyberspace arena.

The ongoing transformation represents a fundamental change – that is, a change in both what is being done and how it is being accomplished. This strategy requires a cultural shift regarding how information and IT are viewed and used.

Information Stewards, Not Owners

Today, there is enormous cultural reluctance to share information with others outside a particular community. Information is considered power, and power is not something to be yielded freely. Information is typically stored in bins and silos that are walled off from those who feel they "own" the information and data. This "need to know" culture is shifting so that we place greater emphasis on understanding who else would benefit by making information accessible. The importance of "need to share" and, more importantly, "right to know" must be recognized. An authorized user, in essence, has the ***right*** to access information that is critical to doing his or her job and in today's information environment we have the technology to provide this capability securely.

To help realize this vision of information sharing, the Department's Data Strategy and Communities of Interest (COI) concentrate on realizing the principles that data must be visible, accessible, and understandable to authorized users. To do so requires "tagging" of data with discovery metadata and enterprise-wide services to enable information to be discovered and exchanged by users (human and machine) as a service within the Global Information Grid (GIG). To enhance the sharing of information among and between

military, federal, state, local, private organizations and coalition partners, COIs are forming across a wide variety of functional domains which allow better exchange of information.

The recent overwhelming success of the Federal Maritime Domain Awareness (MDA) Data Sharing Community of Interest Pilot demonstrates how several executive branch agencies can leverage the early capabilities of the managed services provided by the Department's Net-Centric Enterprise Services (NCES) program to effectively and efficiently share mission critical information. This pilot included the discovery and machine-to-machine sharing of maritime vessel identification, location, speed, course, and destination information among the Navy, the Department of Homeland Security (DHS), the Department of Transportation (DoT) and the Office of Naval Intelligence. The MDA effort also made use of a Google-like federated search capability to advertise, discover, publish, and subscribe to unclassified maritime vessel tracking data. The MDA pilot provided three Federal Departments (DoD, DHS, and DoT) daily access to over 5,000 maritime vessel tracks they previously did not have, and enabled analysts and law enforcement officials to rapidly exploit the new information to better secure our coasts, ports, and waterways. This important net-centric operations capability was delivered in nine months for approximately $1.3 million.

In close cooperation with the Director of National Intelligence (DNI) CIO we are developing a standard, that is, a core vocabulary and data representation, for concepts such as "what," "when," and "where" that are universally understood across the many mission areas of the DoD and the Intelligence Community (IC). These standards are being applied as the basis for the Strike Community of Interest, led by United States Strategic Command, and will enable the multiple agencies and Military Services within that Community of Interest to share and understand critical mission data. The Strike Community is focused on the delivery of joint net-centric command and control and coalition strike planning capabilities that include assets from the IC. Interagency

cooperation between DoD and the IC is essential for sharing critical counter-terrorism and intelligence information among the national leadership, the war planner, warfighter and combat support elements.

Information Enterprise, Not Information Stovepipes

Much of today's information environment is still characterized by stovepipes and systems in which information is, quite frankly, hidden and hoarded, rather than visible and shared. Additionally, many of our existing IT systems cannot talk to each other without the benefit of time-consuming, costly, pre-engineered interfaces. Solutions are based on predetermined needs despite the fact that in today's world it is not possible to anticipate what will be needed or by whom. The challenge is to design, engineer, and create an information environment that can adapt to new users, new technologies and new challenges, rather than one which is static and emphasizes platforms and systems alone. Enterprise services and net-centric solutions are the only way we can overcome these legacy inefficiencies.

To ensure interoperability with legacy systems and ensure end-to-end performance, we are applying extensive enterprise-wide system engineering early in the requirements and decision process. We have established an enterprise-wide systems engineering capability to provide the mechanism by which the Department can collaboratively develop technical interoperability and performance solutions that fosters a truly federated information environment.

Framework for the Future, Not Grand Design

Today's information systems have been developed to retrieve and manipulate data according to very specific and highly tailored requirements. Each organization tends to

pursue its own needs. The result has been a multitude of systems that not only cannot communicate with each other, but are often proprietary, not easily modified and not readily transferable to other needs. To remedy this, we are moving toward enterprise level, end-to-end, lifecycle management of how we design systems and deliver services to the warfighter.

The Department is moving away from a "grand design" systems approach as the basis for its information environment and instead adopting Services Oriented Architecture (SOA) as the key to transforming to net-centric operations. SOA supports an information environment built upon loosely coupled, reusable, standards-based services. It promotes data interoperability rather than application interoperability. SOA ensures providers can reuse what already exists, that is, pieces of applications and data, rather than recreating them each and every time. Moreover, it allows new capabilities to be delivered more quickly. It is allowing the Department to separate data from applications for sharing information within and across the Enterprise Information Environment (EIE).

The second key to success in this area is using commercially managed network services. The Defense EIE will provide commonly available core services; that is, services commonly needed by a wide range of users. Services are required to access, manipulate, share data, and, most importantly, to collaborate across the enterprise. Such core network services must be viewed as resources to manage, rather than applications to be owned. A crucial IT investment for making this a reality is the Department's Net-Centric Enterprise Services (NCES) program, being implemented by the Defense Information Systems Agency. The first managed service, collaboration tools, has been verified and deployed. LtGen Croom will describe in more detail NCES and managed services in his testimony.

Managing Investments by Portfolios, Not Programs

As a result of the 2006 QDR recommendations, the Department is moving to portfolio management, which provides improved management of IT, and other defense resources by ensuring that programs supporting the same capability portfolio are synchronized and that any duplication is eliminated.

For example, the Department has established four Capability Portfolio Management (CPM) pilots with the intent of managing groups of like capabilities across the enterprise to improve interoperability, minimize capability redundancies and gaps, and maximize capability effectiveness. This process is allowing the Department to shift to an outcome-focused model that measures progress by outcomes. The process offers the ability to look at the whole, rather than struggle to determine if there should be a connection between the piece parts. One of the four pilots is the Joint Net-Centric Operations (JNO) capability area, for which I am responsible.

DoD FY08 Information Technology Highlights

As the Department's CIO, I set the policies for the Department's IT initiatives and investments, and I am the milestone decision authority for most of the DoD's major IT investments. Also, my office collects and reviews the Department's IT budget justifications which are ultimately submitted to OMB and Congress. The President's FY 2008 Defense budget request of $481.4 billion represents an eleven percent (11%) increase from what was enacted last year ($432.4 billion), while the Department's FY 2008 IT budget request of $31.5 billion reflects a three percent (3%) increase from what was enacted last year ($30.5 billion). Even though the overall Defense budget has increased due to wartime demands, the IT budget has remained relatively stable. It is critical that we maintain the funding levels requested in the President's Budget to

implement successfully our strategic approach, and progress toward fully net-centric capability that will serve our warfighter and the Department's business functions.

What are we buying with this $31.5 billion?

- Approximately $15 billion in communications and computing infrastructure – including programs such as the Defense Information System Network (DISN), Net-Centric Enterprise Services (NCES), Mounted Battle Command on the Move Program, base-level communications support and infrastructure, and Navy/Marine Corps Intranet (N/MCI);
- Just over $8 billion on warfighting and related national security information systems – including the Joint Tactical Radio System (JTRS), Global Command and Control System (GCCS), Net-Enabled Command Capability (NECC), Forward Area Air Defense Command and Control System (FAADC2), and Mission Planning System;
- Approximately $5 billion in business systems – including the Defense Integrated Military Human Resources System, Navy Enterprise Resource Planning, Defense Travel System, and other Defense Business Transformation efforts;
- Approximately $2.5 billion on Information Assurance initiatives to protect our networks and train our IA workforce; and
- Almost $1 billion on related technical activities such as transition to IPV6, developing technical architectures, and radio frequency spectrum management support.

Defense Acquisition Transformation

Earlier this month the Department provided Congress with our first report on the Department's ongoing Acquisition Transformation initiatives and the goals that we have

established to achieve change. The full report is available at http://www.govexec.com/pdfs/DATR_march7.pdf. The report describes how the Department of Defense is aggressively transforming its institutional acquisition processes and systems to align with 21st Century national security and defense objectives, and achieve a more integrated, cohesive environment. Every aspect of how we do business is being assessed and streamlined to deliver improved capabilities to our warfighters and to provide visibility to our senior leadership. A significant part of this effort entails integrating capability, analysis, and resource processes with periodic review by the Department's Deputy's Advisory Working Group – the DAWG.

Early collaboration on investment decisions among the joint warfighter, acquisition, sustainment, and resource communities is being accomplished through common databases, analytic methods, lifecycle metrics, and networked information sources. This level of in-depth collaboration is new and includes defining requirements in terms of effects-based outcomes and mapping resources according to "joint capability" areas.

IT Acquisition – Initiatives and Accomplishments

We continue to address ways to improve the IT acquisition management and procurement processes that serve as examples of how we are actually transforming the way we do business and delivering net-centric capabilities. These initiatives are aimed at improving results, saving time, and saving money while getting the capabilities, IT services and products in our customers' hands in a timely manner.

We are changing our approach and revising our acquisition model for IT to meet our goal of providing products to our customers, the warfighter, as quickly as possible. Our new process is designed to improve cycle time of our IT acquisitions without losing the discipline of our current process. We are adopting a Time Certain Development process that places a higher priority on schedule than in the past. We will require our IT

programs to change their focus on delivering useful military capability within specified periods of time. To enable this shift we will concentrate on developing and delivering smaller increments of technology within the broader program. These smaller increments will place a higher priority on lower risk, more mature technology. Using this approach, higher risk, less mature technology may be rephased to later increments in the program.

Improving cycle time is key to our new approach. We must also ensure that the operators of the new products are fully trained and that the users have a support infrastructure to rely on when additional help or replacement products are necessary.

Two additional improvement initiatives, risk-based source selection and incentive contract arrangements show a lot of promise. The objective of risk-based source selection is to provide an informed basis for assessing industry proposals, quantifying the risk in terms of time and cost, and enabling more informed discussions with offerors. The results will be more reliable estimates of program lifecycle costs, proposal risk, and improved management and stability.

The use of incentive arrangements in contracts provides motivation for excellence in such areas as quality, schedule, technical performance and cost management. In particular, award fee arrangements are often used when the nature of the work to be performed offers a wide range of potential outcomes, many of which may be beyond the contractor's control. In view of these uncertainties, award fee arrangements are used to motivate the contractor in ways that will result in the best possible outcomes under the circumstances.

Also, the Department is changing the way we procure information technology. These include the DoD Enterprise Software Initiative (DoD ESI), and the federal SmartBUY Program, which is led by the Office of Management and Budget (OMB) and managed by the General Services Administration. Both initiatives seek to establish strategic relationships with key vendors, initially by consolidating the purchasing power of the

DoD and/or the other federal agencies to obtain optimal pricing and preferred terms and conditions for widely used commercial software and related services. The SmartBUY Program often leverages existing DoD ESI resources, including software product management and contracting support, to establish "co-branded" SmartBUY/ESI agreements for use by the entire federal government.

The DoD ESI was established in 1998 to implement a software enterprise management process within the DoD. As an ongoing joint, cooperative venture actively involving 10 separate DoD Components, the DoD ESI started by pooling commercial software requirements to present a single negotiating position to leading software vendors. Twenty-three software best practices were adopted by the DoD ESI Working Group, leading toward a DoD-wide business process for acquiring, distributing and managing Enterprise Software. The DoD ESI has since expanded to include commercial software implementation services from major systems integrators, and information technology (IT) hardware. Agreements are now in place with 37 major commercial software publishers and service providers, yielding substantial (approximately $2.5 billion) cost avoidance for DoD ESI customers . Preliminary work will soon begin on an IT Asset Management Pilot to improve visibility of the commercial software and hardware that comprise a vital portion of the DoD's capabilities. DoD ESI leaders are members of the DoD Strategic Sourcing Directors Board, and contribute to the DoD Strategic Sourcing Report, submitted annually to OMB.

Information Assurance

Information Assurance (IA) – protecting the data and defending the network – is as critical to the Department's Transformation as the data strategy described earlier. The importance of IA to protect the information and infrastructure simply cannot be overemphasized, as evidenced by its selection as one of four Critical Joint Enablers considered in the QDR.

In order to depend on the GIG as the transformational weapon system it has become, we must be confident that the network will be available and we must trust the integrity of the data. To this end, we continue to follow the tenets of the DoD Information Assurance Strategic Plan and emphasize IA policy and systems engineering integration of complex IA capabilities. By doing so the Department ensures IA is implemented and managed across the enterprise in a standardized manner to enhance warfighter and business operations. I would like to highlight six initiatives that are helping to defend the GIG.

- First, we successfully piloted a commercial tool suite with integrated security solutions that will be installed on every computer and server in the DoD beginning in FY 2008. This suite monitors and blocks intrusions at the host level and will be centrally managed at the military service and agency level.

- Second, we are embarking on innovative ways to manage, train, and educate critical IA personnel in the Department. The IA Workforce Improvement Program (IA WIP) establishes specific Department level training, certification, and tracking requirements that Combatant Commands, Services, and Agencies must follow to train and certify the over 70,000 DoD IA workforce members to a common baseline standard.

- Third, I established a priority within my organization to provide technical and non-technical advice on the safeguarding of identities and sensitive information that characterizes people, systems, and services. The Department's identity management approach is composed of three technology-based programs (Public Key Infrastructure, Common Access Card, and Biometrics), which are used to ensure that identities for all entities (humans, devices, and applications) have been successfully authenticated and are properly managed and protected. This, in turn,

increases the reliability and trust of the information provided, and most importantly, increases the overall safety of our warfighters.

- Fourth, my office, in conjunction with the DNI CIO, established the Unified Cross Domain Management Office in order to allow the DoD and Intelligence Community to more effectively share information between security domains—that is, to move information between networks at different classification levels throughout the federal government. This effort and associated technology are important because they govern the ability of federal intelligence agencies to inform state, local and tribal first responders about pending terrorist threats and it, enables information sharing among allies, coalition and other partners.

- Fifth, the Joint Task Force - Global Network Operations (JTF-GNO) continues to conduct an aggressive network defense campaign against growing threats to the Global Information Grid (GIG) by identifying significant threats and developing, disseminating and implementing countermeasures to these threats. LtGen Croom will describe in more detail the activities of the JTF-GNO in his testimony.

- Lastly, we continue to transform IA for the GIG through advanced research. DoD is researching techniques that will help the JTF-GNO to identify more rapidly and react to malicious activities. NSA continues to work on delivering a trusted platform to be used throughout the GIG, and researching secure, high-speed, optical switching techniques.

IT Workforce

One final area I would like to emphasize is our workforce, which is critical to the implementing the net-centric vision and our goals. We are partnered with the

Information Resources Management College (IRMC) of the National Defense University to develop graduate level curricula and programs to meet current and emerging information technology management skills requirements for middle to senior level military and civilian managers within the Department. The curriculum is dynamic and reflects the latest policies, best practices and legal requirements to manage complex IT initiatives, as well as courses in continuity of operations, disaster recovery, national security and military operations, and cyber attack and defense computer laboratory exercises. The programs available provide certificates in a variety of IT disciplines, including IA. Through flexible on-line distributed learning course offerings we are able to get DoD IT professionals certified across the country and while deployed, including in Iraq and Afghanistan.

We have also engaged with our own national agencies as well as with international partners to create a forum where IT problems can be explored and solutions shared. Students from over 20 nations have attended IRMC's Advanced Management Program in residence at Fort McNair. In addition, IRMC has formed international agreements to assist in tailored, IT educational capacity building projects in course development and faculty enrichment with coalition partners such as Bulgaria, Romania, and Singapore.

We continue to recruit talented IA and IT personnel through the very successful IA Scholarship Program. Last year we awarded 23 new IA scholarships to university students and provided grants to universities and colleges to improve their IA research and curriculums. We currently have 75 National Centers of Academic Excellence in Information Assurance Education located in 31 states and the District of Columbia. This is a real success story.

Summary

By now it should be evident that information and IT are critical resources in every aspect of the Department's operations. The net-centric operations transformation will enable the Department to be more effective and efficient. This will provide timely situational awareness that enables superior decision-making by our senior leaders and warfighters and allows them to get into the enemy's decision cycle.

The Department will continue to use the DoD data strategy to improve its information / data sharing across a multitude of domains, ensure that its information is protected and networks defended and secure; and continue to transform the acquisition process so that we can provide the best capabilities and tools for our soldiers, sailors, airmen, marines and those who support our warfighters.

Mr. Chairman, and members of the Subcommittee, I thank you again for the opportunity to speak to you today. We greatly appreciate the support you have given us, and I look forward to our continued collaboration. I would be happy to answer any questions you may have about the Department's information technology initiatives.

Good afternoon, Mr. Chairman (Congressman Smith), Congressman Thornberry, and Members of the Subcommittee. I am Lieutenant General Charlie Croom, the Director of the Defense Information Systems Agency (DISA) and the Commander of the Joint Task Force - Global Network Operations (JTF-GNO). I am pleased to appear before the Subcommittee today to discuss that portion of the Defense Department information technology budget which funds the Defense Information Systems Agency (DISA).

Information is America's greatest weapon system. Rapidly sharing information to ensure the warfighter has the right information at the right place and time remains our goal. Therefore, across the Department of Defense and with our partners in the Information Sharing Environment (ISE), requirements supporting a global, interconnected force demand that we continue the transformation in the way information is managed and shared to accelerate decision-making, improve warfighting, create intelligence advantages, and optimize business processes. Net-centricity is the means by which we will accomplish this. The foundation is the Global Information Grid (GIG), which is the global end-to-end set of information capabilities and services for collecting, processing, storing, disseminating and managing information on demand for the Department.

As stated by the Assistant Secretary of Defense for Networks and Information Integration, net-centricity has four goals:

- Build the net
- Populate the net
- Operate the net
- Protect the net

In pursuit of these goals, the Assistant Secretary has challenged us to accelerate the adoption of a net-centric culture in the Department, make information a force-multiplier, aggressively defend the network, facilitate warfighter connection to all information including intelligence information, achieve agility with non DoD partners, and invest in information technology prudently.

The essence of net-centricity is placing all information – intelligence, command and control, logistics and business information – in the hands of users, allowing them to plug in to the "network" from wherever they are and pull the information they need for their particular mission. We view the network as one including communications, computing, and storage, all provided and managed in a coherent, dynamically scalable and secure manner. Net-centricity will facilitate powerful, immediate decision making based upon machine-to-machine interaction wherever possible.

To achieve net-centricity, the Global Information Grid must be a www-like enterprise in which people can discover information, orchestrate their own operational picture based on the situation at hand, and operate securely in a trusted manner. We must bring people together efficiently, help them do their jobs in ways never anticipated, and enable them to compose services to do things never envisioned.

DISA has a crucial role in moving the Department toward net-centricity. We imagine and envision a world in which information is virtual and on demand with global reach. Information is protected by identity-based capabilities that allow users to connect, be identified, and access needed information in a trusted manner. It is a world in which United States military forces can deploy and connect no matter where they are located, pull information needed for their missions, and be given timely, accurate information on any threats they may face. It is a world with well-developed and available standards and no seams between the sustaining base and the tactical edge. It is enabled by an equally well-developed and available set of standards facilitating the exchange of data. It is a world in which information services, such as voice, data, and video are converged on a mature, technology-fresh, and available Internet Protocol (IP) network. It is a world in which the past differentiation between the network and computing or data processing no longer exists since computing will be done virtually across the entire network. It is a world in which the United States military can freely exchange information routinely with coalition partners and others responsible for the security and defense of the United States. In addition, by partnering with the ISE, we can ensure the Global Information Grid

connects not only the defense and intelligence communities, but homeland security, foreign affairs, and law enforcement - all of our partners in the Global War on Terrorism. The technology employed is agile, adaptive, and capabilities-based. It uses machine-to-machine communication and wireless connectivity, allowing connection regardless of location. And, we imagine and envision a world in which our soldiers, sailors, airmen, and marines are equipped with Information Technologies capabilities and services that are state-of-the-art.

Frankly, achieving our goals is easier said than done. We have several challenges.

Supporting the network, we need an infrastructure that ensures sufficient bandwidth, computing, and storage are available and can be dynamically allocated to deliver information anywhere in the world as missions dictate. This means a global communications network, with sufficient terrestrial and non-terrestrial bandwidth, that can be configured, allocated, and managed end-to-end. If we are to provide this, it is no longer sufficient for components of the Defense Department to provide segments of the network that are independently engineered, acquired, and managed. DISA will work with the Military Services and Defense Agencies to bring coherence to the network. This will include adequate standards, enterprise-wide systems engineering, a common strategy for architecture, a single concept for network operations and configuration control, and situational awareness of the network from the sustaining base to the edge.

The DoD data strategy focuses on making much more information available, often as a service on the network, so that people who might need the information but previously could not get it, have access. It also aims to advance the Department from defining interoperability through point-to-point interfaces to enabling the "many-to-many" exchanges typical of an interconnected environment. The notion of unanticipated users having access to information means a change from a need-to-know access control model to a consumer-driven access control model. Our data must be an enterprise asset that is visible, available, usable, and trusted on the network when and where needed. We need to work diligently to ensure the data strategy is properly enforced.

We need the capability to link producers and consumers of information across all mission areas – warfighting, business, and intelligence. This will be enabled by a set of core enterprise services that include discovery, mediation, and security. Further, we are acquiring a new set of joint command and control capabilities, based on these core enterprise services, to provide warfighters the ability to define and share information specific to the mission at hand.

As another part of the data strategy implementation, certain kinds of software development in the department are embracing this notion of services-on-the-network. Many business processes will soon be constructed as a loosely-coupled composition of these network-based services. This sort of business process construction is called a *service-oriented-architecture* (or SOA), and we believe it will allow for the more rapid evolution of warfighting processes in the department.

We must command and control the network and aggressively defend it. I will address information assurance later on in my testimony.

We must have a capabilities-based approach to acquisition that moves us away from the traditional system and program-centric manner in which the Department acquires today. We must be able to acquire information technology capabilities and services at near Internet speed to put them in the hands of our warfighters such that they have the advantage over our enemies. We will strive to increase the speed and flexibility of the processes we have employed for decades, and we will strive to tailor oversight and governance to be commensurate with risk. And, we will strive to close the gap between the availability of technologies and fielding them for warfighting advantage.

Our final challenge is paying for the advancements we need. Last year, we experienced two cuts from another Committee, a 26 percent cut in Research, Development, Test and Evaluation (RDT&E) in the Network Enabled Command Capability (NECC) and a 7.5%

cut in procurement for the core services provided by the Net-Centric Enterprise Services program. Frankly, those hurt our efforts.

As I mentioned earlier, DISA has as crucial role in providing the capabilities and services essential to net-centric operations and warfare. From my point of view, DISA has four pillars essential to the Department's mission. These are:

1. the underlying network, or the Defense Information Systems Network or DISN;
2. the computing infrastructure provided by our Defense Enterprise Computing Centers or DECCs;
3. the core enterprise services that enable and facilitate sharing information among systems and users;
4. and the programs that enable command and control, today the Global Command and Control System (GCCS) and that enable us to provide combat support information and management, Global Combat Support System (GCSS).

While both are evolving to becoming net-centric, they will be supplanted by the modern Net-Enabled Command Capability for joint warfighting, a truly net-centric, scalable set of capabilities and services which will be web-based and therefore proliferated far wider than the current client-server based GCCS and GCSS systems.

The evolution of the Defense Information Systems Network continues as we integrate the Global Information Grid Bandwidth Expansion (GIG-BE) capabilities into the network, a project I will describe in greater detail later in my testimony. The GIG-BE was delivered on time and within budget, the only one of the original transformational programs to do so. It is designed to service not only the Department's fixed installations, but also to extend transformational communications to deployed warfighters by connecting to another DISA-provided capability, the Teleports. Together, the Defense Information Systems Network, GIG-BE, and Teleport provide a single, integrated communications infrastructure, a key element in providing the virtual, "always on network" I referred to earlier. Just as you replace your personal computer, the Defense Information Systems

Network must replace obsolete technology which is no longer supported by vendors, and that costs money, a challenge the Department is addressing. The network must expand, and contract if need be, to meet changing demands in the world. The establishment of the Africa Command provides a good example of our changing network. This too costs money.

The computing infrastructure and our Defense Enterprise Computing Centers (DECCs) must continue to evolve as well. The private sector has turned to web-based, highly scalable computing platforms that enable businesses and you and I to compose services on demand to meet daily needs. So too must our computing infrastructure provide highly scalable, on-demand processing. However, we must also deal with disadvantaged and disconnected users. We continue to have bandwidth challenges at the tactical edge, and we will for the foreseeable future. We have warfighting units on the ground, at sea, and in the air that are by necessity at times disconnected from the network. Both of these conditions demand that we provide capabilities and services beyond connecting to the "cloud". We must enable disconnected use in bandwidth limited situations through content staging and delivery and solid end-to-end engineering and configuration control.

The pursuit of net-centricity has resulted in the evolution of a number of programs for which the DISA is responsible. They include the Net-Centric Enterprise Services (NCES), and Network Enabled Command Capability (NECC), formerly called Joint Command and Control (JC2).

To help speed the transition to the DoD data strategy and to the Service Oriented Architecture, DISA is developing Net-Centric Enterprise Services (NCES). NCES will provide a set of core services focused on information sharing, enabling data access and the construction of SOA -based business processes. Some of these services will help people find and understand information contained in the services on the network. In addition to these, NCES will provide standards and some core services aimed at enabling the consumer-driven access control I described above. Service consumers and service providers will identify themselves to each other using Public Key Infrastructure identity

credentials, then service providers will check to see whether attributes about the consumer (a person or another computer) show that the consumer should be given access. As examples, these attributes might be associated with a person's role, with a person or a computer's organizational affiliation, or with geographic location. We have published standards for this new form of access control (called attribute-based access control or ABAC), and are partnering with the military services and with NSA to build and use prototype versions.

The Net-Enabled Command Capability (NECC) Program will enable decision superiority via advanced collaborative information sharing achieved through vertical and horizontal interoperability. NECC uses a tailored acquisition approach designed to rapidly deliver a series of smaller, tightly coupled command and control capabilities to implement capabilities as they become available. This new approach is envisioned for development, test, and certification. DISA is defining a highly interactive development and evaluation process called the Federated Development and Certification Environment (or FDCE) to enable agile provisioning of services on the network, and to ensure that service providers and service consumers understand each other's requirements. The Joint Combat Capability Developer (JCCD) for NECC is Joint Forces Command (JFCOM). They will define the "what". The Federated Development and Certification Environment will provide the means; and the Combined Test Force will ensure that capabilities and services can operate on the network and provide warfighting advantage. Per our Adopt before Buy, Buy before Create model, we will leverage existing and emerging capabilities as NECC components. Later this year, DISA will define and pilot a modified certification and accreditation process that will fit into the Federated Development and Certification Environment. As we work out the kinks, I expect this new certification and accreditation process to become the Department standard.

Mr. Chairman, I would be remiss if I did not mention other DISA missions providing critical support to the President and Defense Department. The first of these is the White House Communications Agency or WHCA that provides communications for the President, Vice President, and senior White House staff both on the 18 acre White House

compound and when they travel. We have modernized the capabilities used to support the President over the past five years and we have programmed to continue the modernization throughout the Fiscal Year Defense Plan.

We also provide critical support to the Defense Department through the Joint Interoperability Test Command or JITC and the Defense Spectrum Organization. The JITC provides interoperability testing and certifications for all joint communications and information technology systems acquired by the Department. The Defense Spectrum Organization provides support to the Secretary in ensuring the Department has the radio spectrum frequency agility needed to allow us to operate globally. It also provides technical support to deploying warfighting forces to de-conflict frequency congestion and solve interference problems.

Spectrum is extremely important as an enabler for net-centric operations and warfare. As the Department of Defense (DoD) transforms to net-centric warfighting concepts, the realization of a fully networked and highly mobile battlefield will be increasingly dependent on assured access to the radio spectrum. Consequently, the electromagnetic spectrum emerges as the dominant transmission medium for tactical mobile forces to move information effectively; and, integrate wireless systems into a cohesive part of the warfighting force. Because of the net-centric vision to accommodate and interconnect people and systems independent of time, location, topology, and routing, planning complexity increases to a level such that current processes cannot adequately manage available spectrum. Net-centric spectrum management will provide spectrum support by assuring on-the-move access and interference-free operations. These assurances are the basic tenets of net-centric spectrum management and support achievement of the "ubiquitous, robust, trusted, protected network" envisioned by the DoD. Because of the complexity of the mobile tactical environment, spectrum management must be decentralized and performed autonomously throughout the network to be successful. Achieving net-centric spectrum management will require active participation throughout the DoD and also require direct and continuous liaison with both national and international spectrum entities. Net-centric spectrum management will not be achieved in

the near future, but will evolve as systems, processes and practices assimilate the attributes of net-centricity.

This will require continued refinement as net-centricity matures and will be amended and revised as necessary to assist in assuring the attainment of an operational net-centric environment. DISA is supporting two key initiatives to achieve transparent spectrum access for net-centric: the Defense Spectrum Management Architecture and the Global Electromagnetic Spectrum Information System (GEMSIS).

Mr. Chairman, I believe that we have been highly successful in delivering command and control and combat support systems and their supporting information technology infrastructure. As we move further toward net-centricity, we have initiated programs that will deliver the communications, data processing, and security that will allow us to provide net-centric capabilities and services to our nation's warfighters.

I would now like to discuss our major transformational success as a Joint Acquisition Agency.

DISA has implemented a phased approach for enterprise information technology capabilities and services. The Agency acquisition workforce consists of highly trained and skilled professionals who understand the importance of surety, reach, and speed as components of the Agency strategy. We adopt innovative ideas and processes to deliver capabilities and services to close the gap between the availability of technologies and fielding them for warfighting advantage. In this regard, speed of delivery is often more important than a perfect solution.

We follow the precepts of "adopt-before-we buy" and "buy before we create" based on a best value assessment. If another organization has developed or acquired a capability or service that either fits or is close to fitting a need we have, we adopt it. Where opportunities are not available, we turn to the private sector and acquire a capability or service that either fits or is close to fitting the need. In both cases, we will perform a risk

analysis working closely with the operator to determine if we can realistically use something that delivers less than 100 percent of the need, what elements will not be satisfied, and whether or not they are so crucial so as to preclude adopting either the other government solution or the managed service. We will also determine if a second or third source can be used to provide the critical missing elements and if that course of action is feasible and cost effective. Our final choice is to create or build and we intend to avoid development and turn to others for solutions when we can. We will pursue the "adopt-before-we-buy" and "buy-before-we create" approach as a way of getting the 80-percent quality solution in the hands of the warfighter more quickly.

Consequently, we tailor our acquisition approaches and are developing innovative relationships with industry partners for strong performance-based solutions, speed, risk balance, and mission assurance. The following examples exemplify the use of tailored acquisition approaches.

Our Agency is implementing the DoD Teleport System. This system integrates, manages, and controls a variety of communications interfaces between the Defense Information System Network (DISN) terrestrial and tactical satellite communications (SATCOM) assets at a single point of presence. The system is a telecommunications collection and distribution point, providing deployed warfighters with multi-band, multimedia, and worldwide reach-back capabilities to the DISN that far exceed current capabilities. This new system provides additional connectivity via multiple military and commercial SATCOM systems, and it provides a seamless interface into the DISN. The Teleport Program employed an evolutionary acquisition approach designed to maximize use of commercial off the shelf technology to provide capability to the warfighter as quickly as possible. The program is being incrementally fielded in generations, with each generation further broken down into capability increments. By maximizing existing technology, the program entered Generation 1 at Milestone C. We are working with the Services to take advantage of their expertise. For example, we are leveraging the Navy's UHF, EHF, and Teleport Management and Control Segment (TMCS) capabilities and the Army's Ka, IP, and Baseband capabilities.

Within the Commercial Satellite Communications program, we are proactively improving commercial SATCOM for the warfighter. The program office has cut provisioning timelines down from (as reported in a GAO report) a 79 day average to the current median of 21 days. Contracting and engineering fees have been reduced from 8% to 3.41%. Customer satisfaction ratings (using a 5 point scale) have increased from 3.9 in fiscal year 2005 to 4.5 in fiscal year 2006. In addition, business process reengineering is underway using the Lean Six Sigma model.

The Net-Centric Enterprise Services (NCES) Program is employing acquisition streamlining and speed of delivery concepts that include managed services provided by government and/or commercial industry. We execute accountability and service delivery using performance agreements such as Memorandum of Agreements, Service Level Agreements, and Performance Work Statements. We use broad Statements of Objectives supplemented with NCES specifications to communicate requirements. The service provider is responsible for life cycle management. Early user testing combined with developmental testing, demonstrations and operational assessments are used to identify gaps and provide information to support Limited Operational Availability (LOA) decisions. LOA decisions afford a declaration of user confidence to determine a capabilities ability to support a specified user base. LOA decisions also provide useful capability during the System Development and Demonstration Phase and assessment criteria based on service/capability type and associated risk.

As I mentioned earlier, the Net-Enabled Command Capability (NECC) program will use the enterprise services provided by NCES and will lead our efforts in streamlining acquisition of services and capabilities. I'd like to re-emphasize that NECC uses a tailored acquisition approach designed to rapidly deliver a series of smaller, tightly coupled command and control capabilities implement capabilities and services as they become available. This new approach will couple users, developers, testers, and certifiers in concurrent development, test, and certification. Again, we call this the Federated Development and Certification Environment, or FDCE.

As I said earlier, we will continue to develop innovative relationships with our industry partners. One example that we discussed earlier was the managed services concept employed by the Net-Centric Enterprise Services (NCES) program. We are also employing a capacity-on-demand services concept to acquire data processing and storage as services provided by vendor partners on our data center floors. We pay only for the capacity that is needed. This approach has the benefits of reduced time to add capacity, simplified cost drivers, streamlined operating system management, and facilitated technological currency. It is our intent to expand the concepts as appropriate to other capability requirements.

The Department of Defense has allowed DISA to tailor acquisition processes and use industry partnerships to accelerate providing capability to the warfighter. From an acquisition perspective, we believe our major challenge is clear. Specifically, we need to continue to accelerate speed of delivery, embrace risk-based testing, right-size the information assurance (IA) certification, support streamlining the requirements process, and support timely decision making as embraced by the Under Secretary of Defense for Acquisition Technology and Logistics in the Lean Six Sigma approach to streamline acquisition oversight. All these actions are required to reduce cycle time so that capability can be delivered to the warfighter inside the proverbial 18 month information technology change window. Capability must be deliverable before technology changes.

I'd like to turn now to Information Assurance.

Our efforts at DISA and at the JTF-GNO in information assurance are aimed at achieving two fundamental department-wide goals. First, DoD missions must continue to function well in spite of a cyber attack against the department's information infrastructure. Second, the department and its partners must be able to keep a secret when we need to, while at the same time being able to share information as broadly as possible. These are tough goals given the enormous complexity of the department's infrastructure, and can only be achieved by coordinated effort amongst all DoD entities responsible for acquiring

and operating portions of the information infrastructure. Clearly information assurance is a team sport, and we are teamed with the combatant commands, the Joint Staff, the Office of the Secretary of Defense, the military services, the National Security Agency, and many other department, federal, coalition, and industry partners in our efforts.

As JTF-GNO Commander, I am responsible for operating and defending the Global Information Grid (GIG). This responsibility flows from responsibilities given to the United States Strategic Command. Like any JTF commander, I have component forces from each of the military services.

DISA has several core roles in DoD information assurance. One is to ensure that the products we provide have appropriate security built into them. An example of this is the security being built into the Net-Enabled Command Capability program. A second role is as a provider of many of the core standards, processes, products, and services necessary to the establishment and maintenance of cyber defense-in-depth, and cyber attack detection and reaction capabilities across the department. In this DoD-wide role, DISA is teamed closely with the JTF-GNO. I would like to focus on that role here.

I will start by describing what we're doing to help DoD achieve the basics of information assurance, then I'll describe how our efforts are changing to anticipate and adapt to ongoing changes in DoD initiatives and to changes in information technology. Our programmatic efforts are done as part of the overall DoD Global Information Grid (GIG) information assurance portfolio, or the GIAP.

The basics start with secure configuration. This means ensuring that every device in the information infrastructure is configured as securely as possible. It also means that as vulnerabilities are discovered, device configurations are updated and devices patched as quickly as possible, and that the right people know the state of configuration of the infrastructure.

Secure configuration of devices starts with someone determining what a secure configuration actually is. DISA is partnered with the National Security Agency, with the National Institute of Standards and Technology, and with industry and non-profit entities in the production of guidebooks that describe the proper configuration of a particular operating system, for example. The DISA guides are called Security Technical Implementation Guides (STIGS) and are used throughout the department and elsewhere.

Discovery of a new vulnerability will often trigger changes to these standard configurations. The JTF-GNO tracks vulnerabilities, and when one is discovered that poses significant risk to the department, the JTF-GNO will issue an information assurance vulnerability alert, or an IAVA. An IAVA directs that certain remediation actions be taken by all in the department who administer systems, and directs that all units report compliance with the IAVA. On the unclassified and secret networks, DISA maintains web sites that contain the patches for operating systems and applications that system administrators require in order to comply with IAVAs. These sites ensure that DoD system administrators can get patches from a DoD entity, without having to compete with others on the Internet for access to vendor sites. DISA also acquires and operates a system used by DoD organizations to report compliance with IAVAs and other orders given by the JTF-GNO.

Proper configuration of a complex operating system is very difficult, as is manual verification of compliance with the configuration standard. To help system administrators determine the specifics of a device's configuration, and to help automate the process of changing configuration, DISA has acquired enterprise licenses for a configuration scanning/vulnerability scanning tool and for an automated remediation tool. We did these acquisitions under the oversight of the Computer Network Defense Enterprise Solutions Steering Group, an entity chartered jointly by the ASD (NII) and by USSTRATCOM, and co-chaired by the JTF-GNO. JTF-GNO mandated the use of these tools throughout the department, with the scanning tool as the first priority. The military services field and use the tools, with DISA providing fielding support.

Going forward, we are working with the National Institute of Standards and Technology and the National Security Agency to define industry standards for the description of vulnerability, of configuration, and of compliance measurement and we will then both produce our guidance documents to these standards, and we will purchase enterprise tools that comply with these standards.

In 2006 under the auspices of the Computer Network Defense Enterprise Solutions Steering Group, DISA let a DoD-wide contract for a tool that we call the Host-Based Security System, or HBSS. This is a piece of software that will sit on most computers in the department and will do a number of things associated with securing and reporting on these computers. Here are a few examples. The Host-Based Security System will further harden these computers against attack, including certain kinds of attack that have never been seen before but that are related to well-understood classes of vulnerability. It will also allow signatures that protect against emerging or rapidly spreading attacks to be pushed quickly to these machines. Going forward, it will also help to bring a machine back to a well understood configuration baseline, and thus remove malicious software that was not part of the baseline. The Host-Based Security System is being piloted at more than 20 sites throughout the department and will begin broad deployment later this spring.

Another part of the basics of information assurance is the provision of perimeter defenses for enclaves of computers. DISA builds and operates the primary perimeter defense between the DoD and the Internet as part of the overall Internet/DoD gateway system that DISA provides. This system is under the direct operational control of the JTF-GNO. The policy for what passes through this perimeter and what does not is set by the JTF-GNO and can be changed rapidly in response to changing threat conditions or other mission needs.

Most computers in the department are protected by several layers of perimeter defense, including the outermost one I just described. Some of these defenses are at the boundary between a military base and the department's core networks; some of these defenses are

located at the boundary between a tenant organization and a base; and still others are at the satellite communication gateways to deployed forces, or located in the deployed enclaves themselves. Policy at these shared perimeters defenses must be harmonized across the entire department to ensure that appropriate security is maintained while at the same time joint applications and business processes are not hampered by a local perimeter policy decision.

The JTF-GNO directs the perimeter policy at all large shared perimeter defenses in the department, supported directly by a DoD-wide risk management process run by DISA called "ports and protocols." The risks to computers inside an enclave of a particular network protocol are analyzed by DISA, and then a recommendation on whether the protocol should be allowed or denied is made to the DoD-wide risk management jury called the DISN Security Accreditation Working Group (or DSAWG). DISA chairs the DSAWG, with participation by the Combatant Commands, Services, Defense Agencies, and the intelligence community. The DSAWG's recommendations are forwarded to the JTF-GNO.

In order to shield most computers in DoD from direct attack from the Internet, in 2007 we will partner broadly to change the structure of perimeter defenses and of certain applications in the unclassified network. This effort will involve defining access zones in the network. Some of these zones will be visible to the outside world, some only to close partners, and some will have very restricted access. As part of the server consolidation going on in the military services, we will begin the movement of all publicly-visible and partner-visible servers into these more publicly visible zones. In cyber security jargon these more public zones are called demilitarized zones or DMZs. The servers in the DMZs will then act on behalf of the partner or on behalf of the public, and will reach back into the more restricted zones when necessary. This design is very similar to that used in large e-commerce companies to provide a rich customer experience while still protecting the back-end finance, inventory, and personnel databases. I expect that the application transition into DMZs will take several years. While we are moving to DMZs,

we are also modifying the design of the domain name system (or DNS) in the department, again to engineer what DoD looks like to the outside world.

A third part of basic information assurance is the use of strong, non-forgeable cyber identity credentials in information system access control, and in the signing and encrypting of documents and email.

Under the auspices of the NSA program manager, DISA acquires, operates, and sustains the DoD public key infrastructure (the DoD PKI). This infrastructure is used to issue two-part cyber identity credentials to all department uniformed, civilian, and on-site contractor personnel, and also provides a service somewhat analogous to a credit card checking service that allows an entity to check the revocation status of the credentials. The public part of the credential is distributed via a directory service that is part of the Public Key Infrastructure (PKI).

DISA and NSA have teamed with the Defense Manpower Data Center to issue the PKI credentials as part of the Common Access Card, or CAC, the standard DoD physical identification card. When someone gets a CAC, they also get both pieces of the PKI credential (the public half and the private half). The chip on the CAC protects the private half of the credential. DoD has issued more than 12 ½ million CACs, and since each CAC has multiple PKI credentials, more than 30 million PKI credentials have also been issued. The military services have deployed CAC readers and the associated middleware to most computers in the department.

As a means of reducing the department's vulnerability to password theft, last year JTF-GNO ordered that all logons to unclassified DoD computers be done via the PKI credential on a CAC. When a person logs in, the person inserts a CAC, then types a number to unlock the private half of the PKI credential on the CAC. The authentication service on the computer, or elsewhere on the network checks that the credential has not been revoked, then uses the public half of the credential to verify the private half. When these checks are satisfied, and if the person is an authorized user of the computer, access

is granted. No password is sent over the network, or stored anywhere other than on the CAC. This, combined with the fact that a physical CAC must be present to log in eliminates some methods of attack and makes others much harder. As of March 2007, 92% of logons to unclassified computers in the department were done using this method.

Additionally, all web servers on the unclassified and secret networks have PKI identity credentials. This year the JTF-GNO will require the use of a person's PKI credential to access "private" unclassified DoD web sites. Since both the person and the web site have PKI credentials, both can verify the authenticity of the other, all without passwords. This will improve security for the information contained in the web sites, and should also help ensure that the end-user is dealing with a genuine DoD web site.

In 2006, the JTF-GNO also directed an increase in the Information Condition, or INFOCON, of the department. As part of this, the JTF-GNO directed implementation of a package of initiatives intended to reduce vulnerability to certain types of attack even further. The most visible of these initiatives was the direction to stop allowing DoD personnel to use a web interface to access their DoD-email. This direction was a result of the fact that most web-based mail systems can only use a user name and password for access, not the stronger CAC/PKI combination. Like all JTF-GNO orders, the web-mail order was first issued as a warning order, and comment on the mission effect from the order was invited from all in the department. The JTF-GNO considered this input, and then issued the final order. Like most broad JTF-GNO orders, this order contained a safety net; exceptions to the policy could be made by people at the three star level or higher. Few of these exceptions have been granted, and DoD has become much more resistant to password-guessing attacks directed at web mail.

We measure compliance with all these initiatives in several ways. First, the JTF-GNO gets reporting on compliance from their components, and from the other organizations of the department. Second, DISA sends teams, under the direction and sponsorship of the JTF-GNO, to selected sites throughout the department. These teams are called Enhanced Validation Visit teams, and report their findings both to the site visited and the JTF-GNO.

The findings are used to correct deficiencies at particular sites, and are also used by various DoD entities to understand systemic programmatic or operational problems.

In spite of all the emphasis on the basics, we know that our defenses will not be perfect, and that vulnerabilities will be found and exploited. As a consequence, DoD also requires the ability to spot attacks, then determine enough about the attack that militarily useful courses of action can be developed, selected, and executed. DISA and NSA acquire and operate attack detection and diagnosis systems at the gateways between the Internet and the DoD. Many attacks that traverse these gateways can be spotted and understood using these systems. The JTF-GNO is the primary customer of the output of these systems, although the information is used by network operations, or NetOps, personnel throughout the department.

DISA and the military services also operate attack detection and diagnosis systems within the department's networks. The DISA Theater NetOps Centers (TNCs) use the DISA-managed detection and diagnosis systems, along with reporting from the NetOps centers of the military services and the NSA, to provide a consolidated incident detection and reporting service to the various combatant commanders. These DISA TNCs are under the operational control of the JTF-GNO, and like the JTF-GNO, the TNCs combine network management and computer network defense personnel to provide the fastest problem diagnosis and resolution possible. These combined centers can more quickly do the triage associated with the question, "Is this a cable cut or a cyber attack?" for instance. The NetOps centers of the military services, as well as the TNCs, all report to the JTF-GNO, which consolidates the global view of incidents and coordinates responses across organization boundaries as required.

Like much other information technology in the department, the attack detection and diagnosis systems used by the military services and DISA were developed and deployed separately, since each organization had a different span of control. Under the auspices of the Computer Network Defense Enterprise Solutions Steering Group, DISA produced a consolidated DoD-wide plan for an enterprise sensor grid last year, and is currently

coordinating a broader attack detection and diagnosis plan which we expect to issue later this year. Additionally, we are pursuing an enterprise acquisition for insider threat observation and detection tools this year. The increased use of public key identity credentials, combined with such tools will allow us to construct a more capable insider threat detection and deterrence capability.

To ensure that the DoD standards for certain NetOps functions are well understood and followed, the JTF-GNO sponsors the Computer Network Defense Service Provider accreditation process (the CNDSP). Teams from DISA and from NSA evaluate operational entities throughout the department to a set standard, and then USSTRATCOM accredits organizations that meet the standard.

How are we doing? First, we are seeing improvements in the configuration of DoD computers. As a result of our configuration automation efforts, and as a result of increased management focus throughout the department, IAVA compliance climbed 136% from June 2006 to January 2007.

We are also seeing more reporting of cyber incidents in the department. In 2004, we had roughly 16,000 incidents reported. In 2005, this rose to roughly 23,000 incidents. In 2006, this increase continued, with a total of 30,000 incidents reported. A cyber incident is an assessed occurrence having actual or potentially adverse effects on an information system. The incident numbers I gave do not include the high amount of scanning data -- roughly 4 times the numbers I just stated. I attribute these increases in reporting to our emphasis on better reporting, and on better operational procedures and technology for detecting attacks. I'd like to emphasize that a major portion the majority of these incidents are *unsuccessful* attacks.

The number of successful attacks declined from roughly 130 in the month of January 2005 to roughly 40 in January 2007. I attribute this decrease to improved configuration control of computers, including that of web servers; the elimination of many passwords, and our focus on perimeter security. A subset of the successful attacks is the number of

DoD computers used in botnets. A botnet is a large network of compromised computers that is typically rented to the highest bidder. Botnets are typically built using completely automated attacks. While botnet activity in the Internet increased roughly 110% from February 2005 to December 2006, during the same period, the number of DoD computers used in botnets *decreased* by 61%.

One more trend I'd like to mention. Our hardening efforts are changing the behavior of certain adversaries. As configuration, password, and some network vulnerabilities are going away, attackers are moving "up the stack" and focusing on data-driven attacks. An example of this is the increase in bogus electronic mail attacks, sometimes apparently coming from a legitimate source. We went from three email attacks reported in January 2006, to a high of 161 email attacks reported in September 2006. This declined to 61 reported attacks in December 2006 as we directed that everyone in DoD be trained to recognize and counter these attacks, and as access to web-mail declined.

Thank you, Mr. Chairman and members of the subcommittee for inviting me to testify before you today. That concludes my formal testimony and I would be happy to answer any questions to the best of my ability.

DOCUMENTS SUBMITTED FOR THE RECORD

MARCH 28, 2007

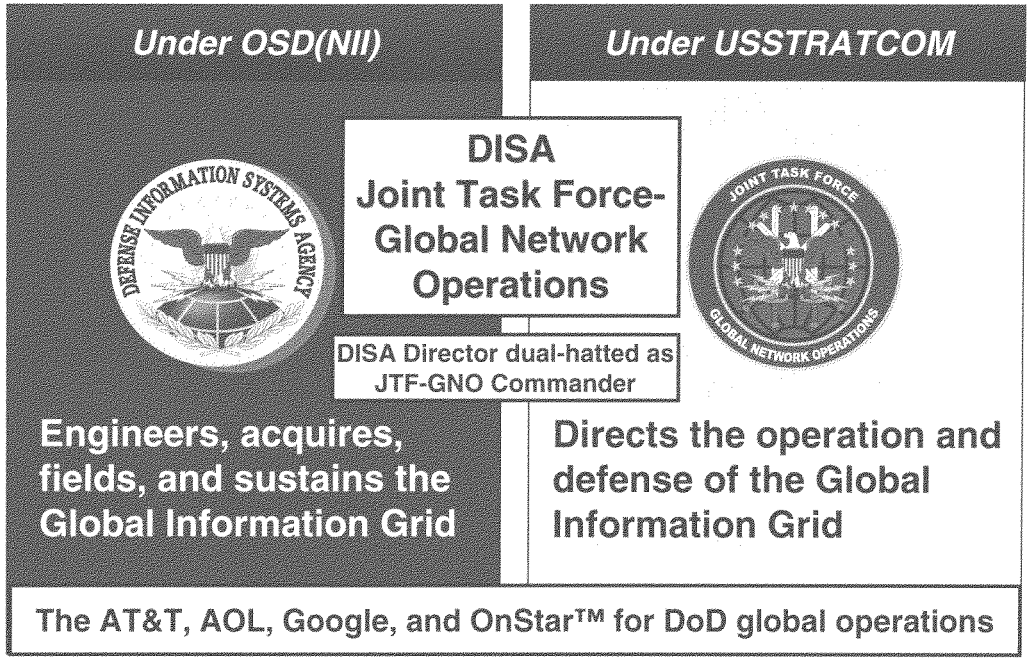
Defense Information Systems Agency
Department of Defense

Defense Information Systems Agency

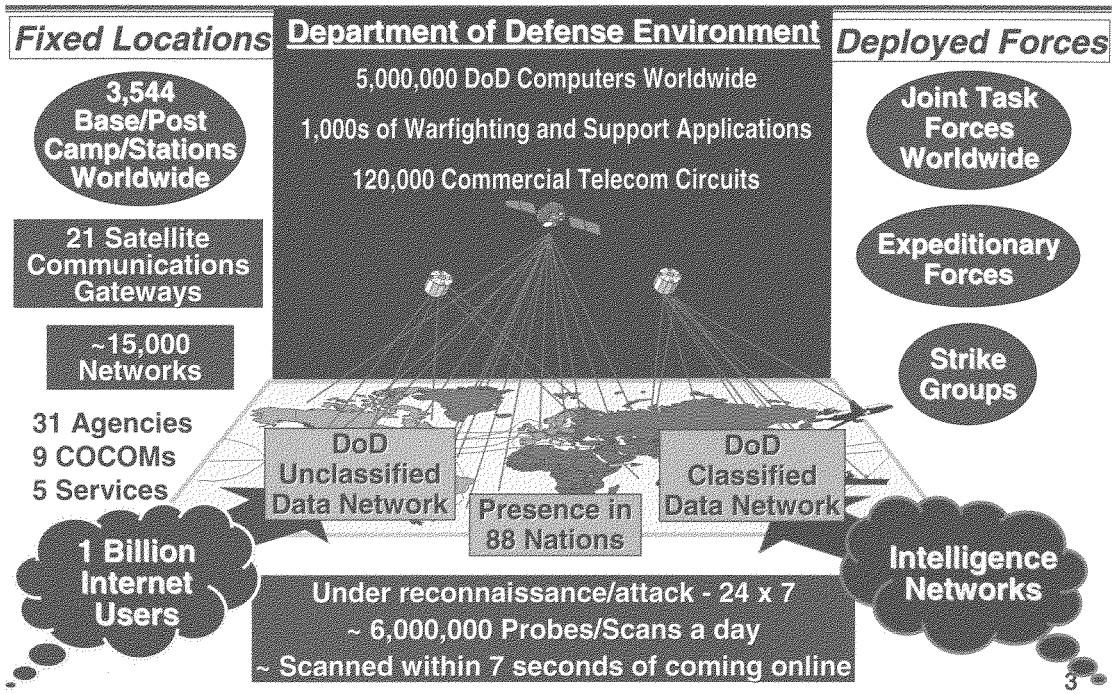
Lt Gen Charlie Croom
Director, Defense Information Systems Agency
Commander, Joint Task Force-Global Network Operations
March 28, 2007

A Combat Support Agency

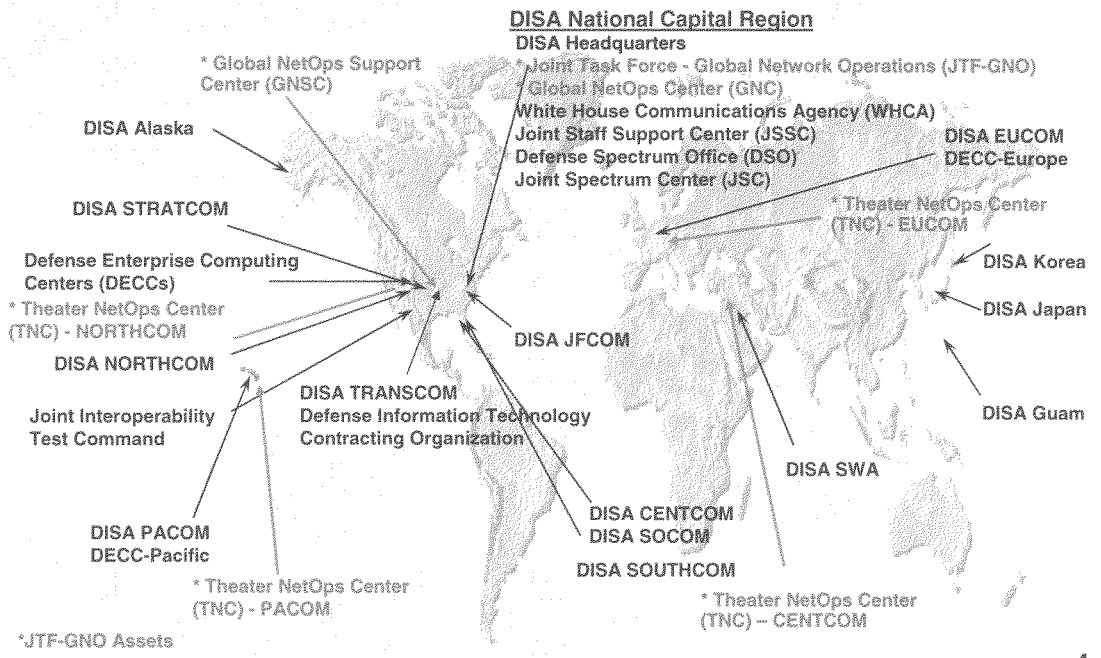
Interlocked Missions



DISA Unique & Dynamic Environment



Global Presence



Special Missions

White House Communications Agency (WHCA)
White House Situation Support Staff
Connectivity for the Commander-in-Chief

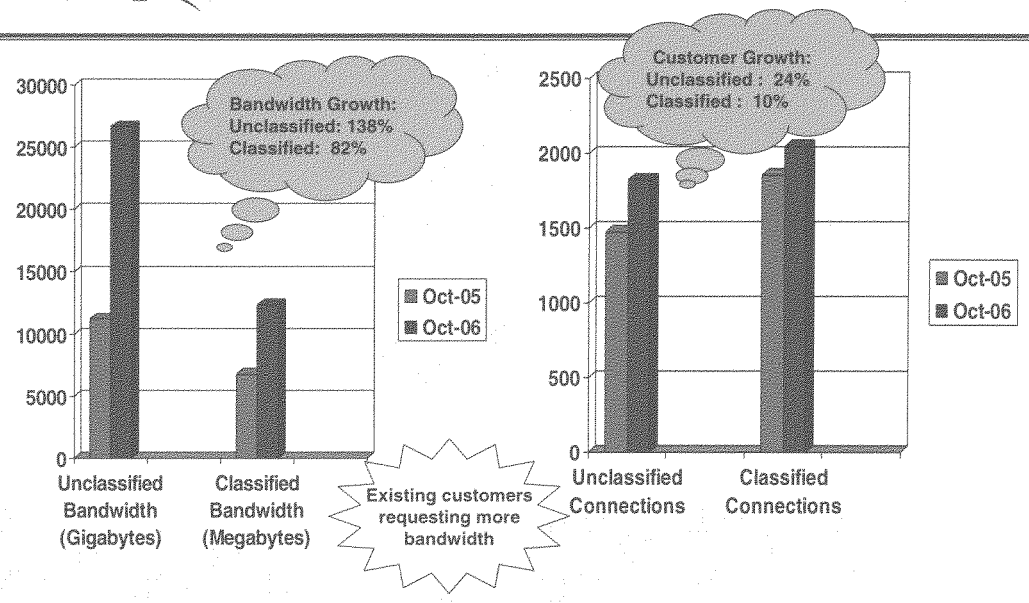
Joint Staff Support Center (JSSC)
Connectivity for the NMCC and Joint Staff

Defense Spectrum Organization (DSO)
Spectrum management and allocation

Defense Information Technology Contracting Organization (DITCO)
Contracting for information technology

Joint Interoperability Test Command (JITC)
Interoperability testing and certification

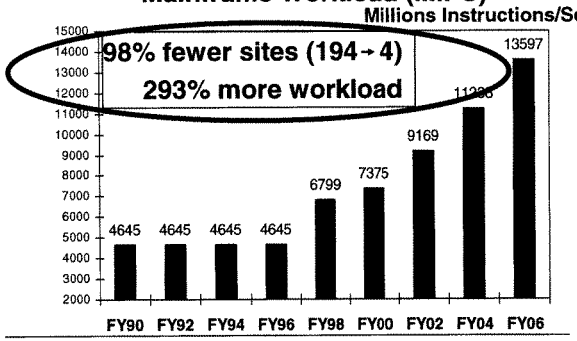
Network Growth



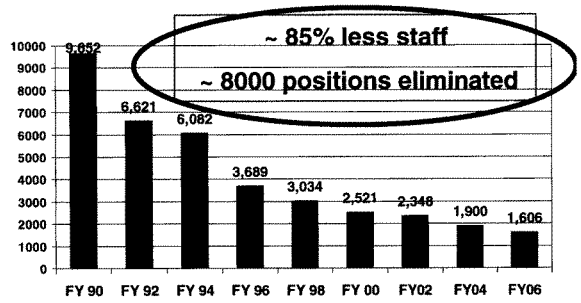
Investment paying off – Global Information Grid-Bandwidth Expansion

Accomplishments: Computing Transformation

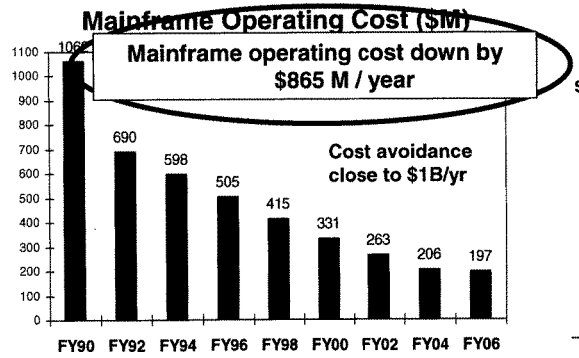
Mainframe Workload (MIPS)



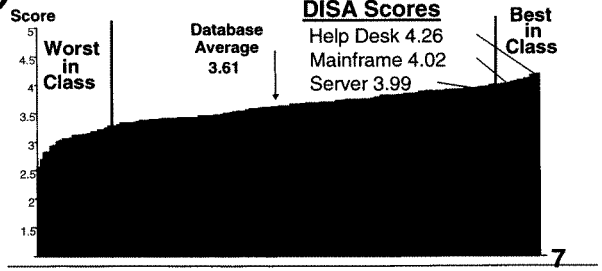
Government Personnel End Strength



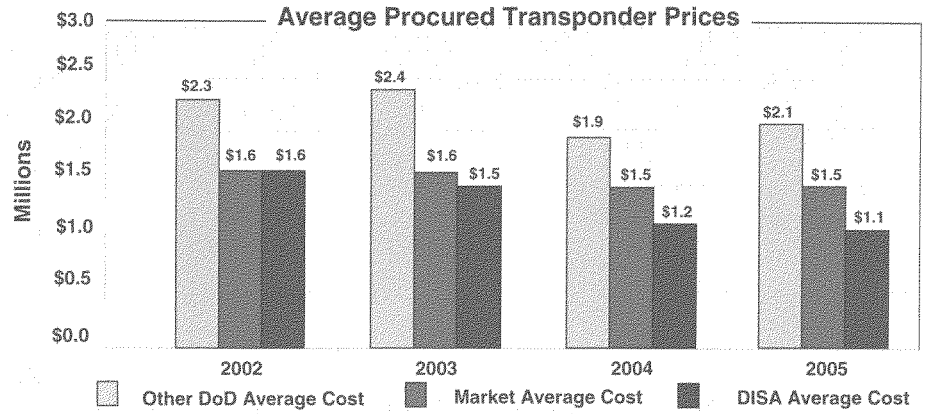
Mainframe Operating Cost ($M)



Gartner Customer Survey "Best in Class" Against Industry



DISA Commercial Satellite Services



- Leveraging DoD buying power: prices now 25% below industry average
- Reduced DISA fee structure: from 8% to 3.41%
- Reduced time-to-service: since 2004, 73% reduction – now median is 21 days, targeting 4 hour emergency response

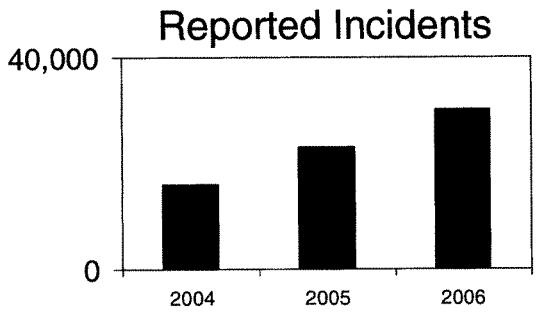
Goal: Mission Assurance

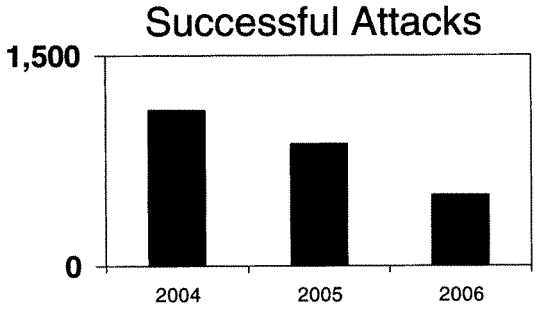
Vulnerability Reduction

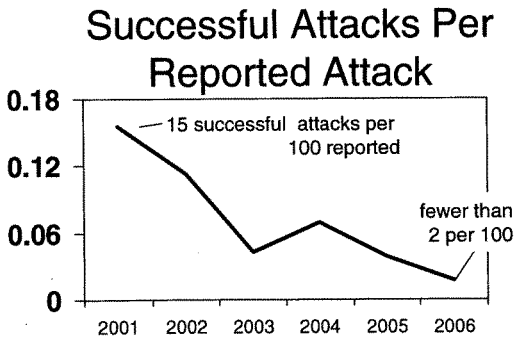
- **Standards and configuration management: configuring each device securely and keeping it that way as new vulnerabilities and attacks appear**
- **Layered defense: standardizing layered perimeter defenses for sharing and security**
- **Identity management: issuing and using standard, non-forgeable cyber identity credentials**

Mission execution in the face of cyber attack

DISA How Are We Doing in IA?







- **Increasing**
  - **Attacker sophistication**
  - **Number of attacks**
- **Improved IA**
  - **Successful attacks declined by 54% from 2004 to 2006**
  - **Declining number of successful attacks per reported attack**

Acquisition – It's All About *Speed*

- The ABCs – adopt before buy, buy before create
  - Adopt less than 100% solutions where appropriate
  - Leveraging commercially available services and commercial practices
- Think big, build small, scale fast – the Google model
  - Small, loosely coupled capability modules
- Paralleling acquisition processes
  - Users, developers, testers, and security certifiers working in parallel
  - Collaboration in a common, virtual development environment
- Tailored acquisition approaches
  - Managed services, service level agreements, statements of objectives
    - Our collaboration services
    - Processing and storage capacity on demand with utility pricing
- Requirements and documentation streamlining
  - Reduce size and time to prepare

Working within the DoD Acquisition Framework

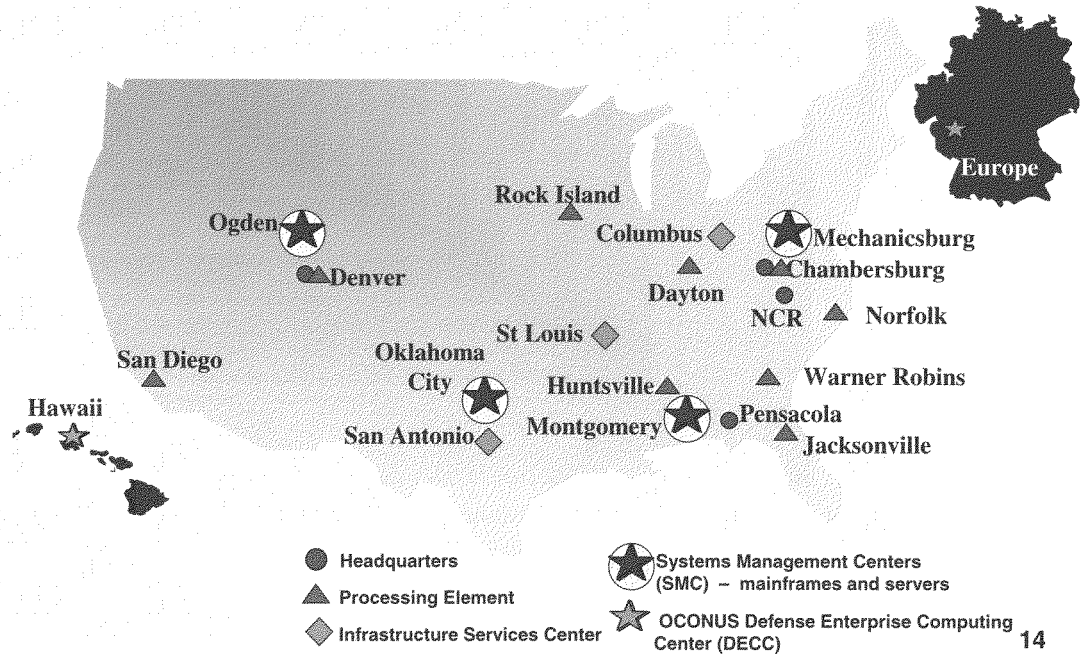
Summary

- DISA provides DoD's global capabilities and services
  - The DoD network – engineer, acquire, implement, manage
  - Network operations and defense – supporting US Strategic Command
  - DoD enterprise computing – pay, medical, logistics, transportation, finance, command and control
  - Core enterprise services – enabling "behind the glass"
  - Global command and control infrastructure
- We are
  - Extending capabilities and services to the tactical edge
  - Working to speed acquisition and using smart sourcing, e.g., commercially managed services
  - Working toward enterprise engineering, testing, certification, accreditation

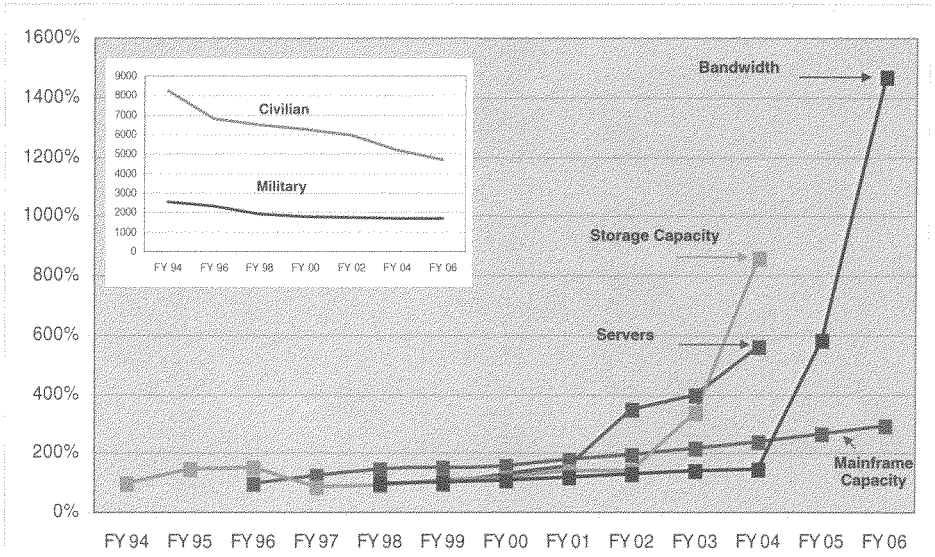
Enabling employment, deployment, and sustainment of warfighting forces


DEFENSE INFORMATION SYSTEMS AGENCY

DISA Computing Services Footprint

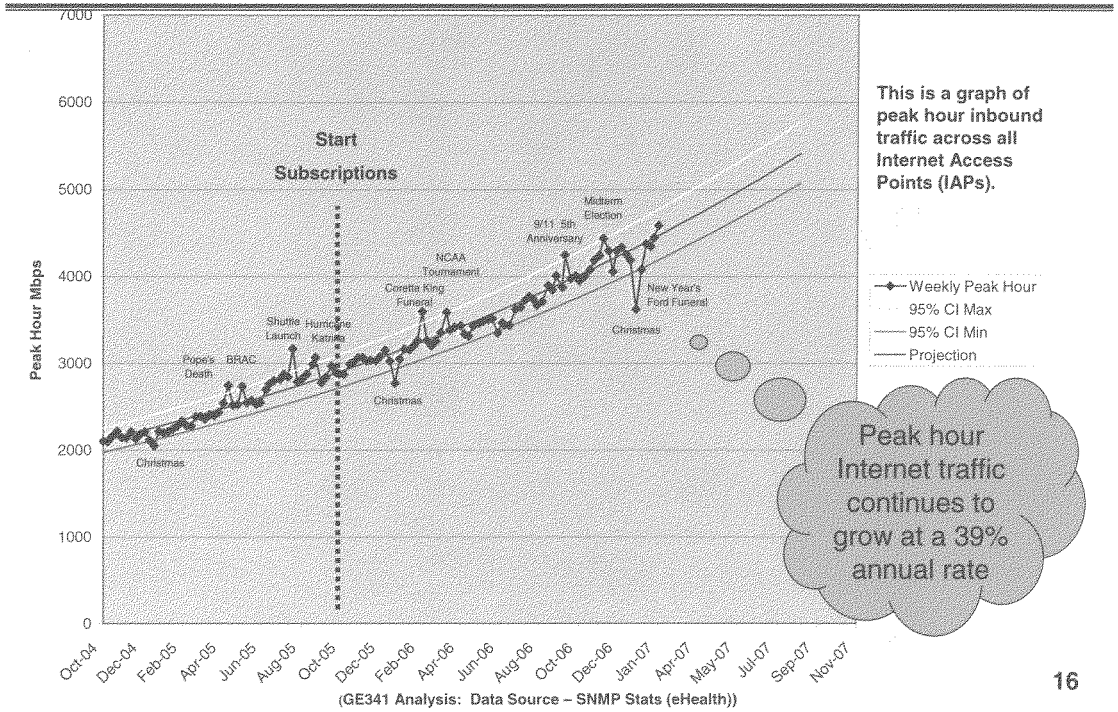


People vs Capabilities



Capacity up – staffing down

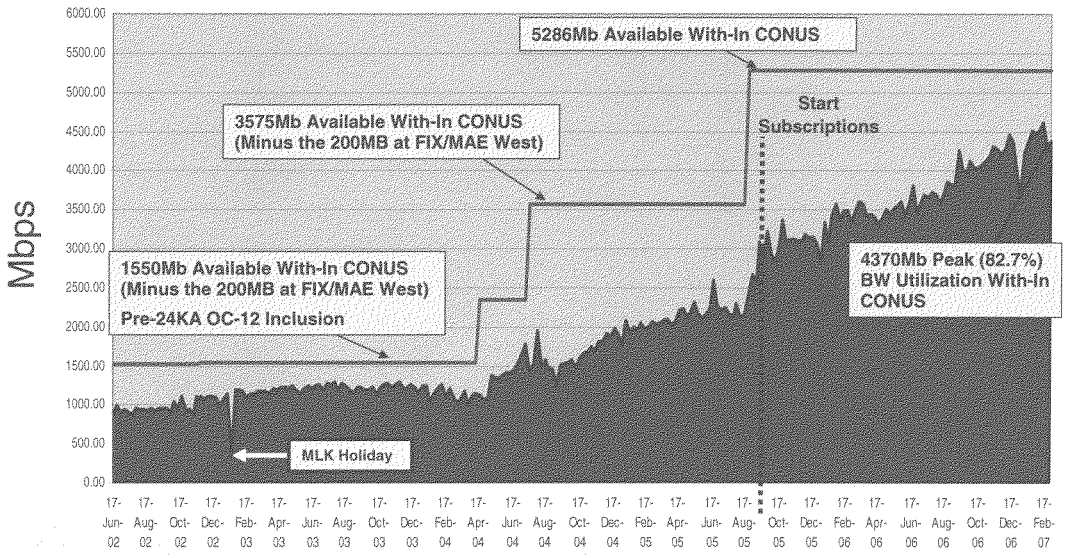
DISA Inbound Internet Traffic Growth



(GE341 Analysis: Data Source – SNMP Stats (eHealth))

NIPRNET Data Performance
(Internet BW Available vs Utilization)

17 June 2002 – 26 February 2007



Intra-CONUS

Information Assurance:

DISA and the Joint Task Force for Global NETOPS are teamed

1. Assured DoD mission execution in the face of cyber attack
2. Ability of DoD to keep a secret while simultaneously sharing information broadly

JTF GNO's mission: Direct the operation and defense of the Global Information Grid to assure timely and secure Net - Centric capabilities across strategic, operational, and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence, and business missions.

DISA's IA roles: Defining DoD-wide enterprise designs and enterprise standards; acquiring, operating and helping to deploy enterprise tools and capabilities; operating enterprise processes, performing validation of compliance with operational and policy standards; operating regional NETOPS centers in support of the JTF GNO and COCOMs; ensuring all DISA products and services have appropriate IA

Vulnerability Reduction

1. Configuring every device securely and keeping it that way as new vulnerabilities and attacks appear

2. Standardizing **layered** perimeter defenses for sharing and security

3. Issuing and using standard, non-forgeable cyber identity credentials

4. Information Condition (INFOCON) increase
   - **Webmail restrictions**

5. Validating compliance

DISA Operational Improvement

- JTF GNO is top operator
  - **Improved info-sharing with key mission partners**
  - **Shared situational awareness with DOD & beyond**
  - **Established operational "sense" of the network**
- Military services, DISA, NSA, field attack sensing systems
- JTF GNO, military service NETOPS components, and DISA theater NETOPS centers use the infrastructure
- DoD-wide enterprise sensor grid plan with new DoD-wide attack detection and diagnosis plan mid-spring this year
  - **Insider threat detection and diagnosis enterprise-wide acquisitions by DISA this year and next**
- JTF GNO, NSA, DISA computer network defense service provider accreditation program

88

Vulnerability Reduction Details (1)

1. Configuring every device securely and keeping it that way as new vulnerabilities and attacks appear
   - **Defining the secure configuration (configuration guides)**
     - Partnering with NIST, NSA, Industry to produce
   - **Deploying the secure configuration**
     - Work with industry so DoD can buy standard configurations (Air Force standard configuration with Microsoft for example)
     - Gold disk tool to configure a system automatically
     - Enterprise-wide deployment of configuration scanner
       - Help system administrators confirm inventory and proper configuration
       - DISA purchases, JTF GNO directs DoD-wide deployment
   - **Maintaining the secure configuration**
     - Information Assurance Vulnerability Alerts (IAVA) by JTF GNO
     - Enterprise-wide deployment of configuration change tools
       - Help system administrators deploy patches and configuration changes (DISA buys, JTF GNO directs deployment)
     - Patch servers on the unclassified and classified networks
   - **Improving automation**
     - NIST/NSA/DISA partnership on industry data standards for vulnerability, configuration, reporting
   - **Training for system administrators**
   - **Adding supplemental protections to key operating systems**
     - Enterprise tools for antivirus, antispyware, and host-based intrusion prevention and baselining
       - Host-based intrusion prevention/baselining in pilot phase; DoD-wide deployment starts this summer.

Vulnerability Reduction Details (2)

2. Standardizing perimeter defenses for sharing and security
   - **Ports and protocols**
   - **Moving all publicly and partner-visible servers into demilitarized zones at the boundary between DoD and the outside world**
   - **Modifying the DoD domain name system to improve performance, yet limit the information about DoD available to potential attackers**
3. Issuing and using standard, non-forgeable cyber identity credentials throughout the information infrastructure
   - **DoD public key infrastructure (PKI) issues credentials as part of the DoD common access card (CAC)**
     - 12.5 million CACs with 28 million PKI credentials issued
     - 3.6 million active CACs
   - **JTF GNO direction to use CAC/PKI for all network logons on the unclassified network to reduce password vulnerabilities**
     - 92% of DoD logging on with CAC
   - **Use on PKI credentials for web servers, JTF GNO soon to require "private" DoD web servers to require PKI certs from customers**
4. Information Condition (INFOCON) increase by JTF GNO
   - **Further tightening of the department's systems**
   - **Like most JTF GNO orders, warning order first, then after comments from the field, final order**
   - **Biggest step was strong restriction on access to webmail to reduce vulnerability to passwords and to socially engineered email**
5. Validating compliance with all of the above
   - **Enhanced compliance validation visits to DoD sites**
     - **GIG vulnerability alerts by JTF GNO**
   - **Reporting via the automated tools above**

How Is DoD Doing in Information Assurance?

- 92% of DoD unclass users logging in using DoD PKI certs on the CAC
- Incident detection and reporting improved
  - 88% increase in reported incidents from 2004 to 2006 (From about 16,000 incidents to about 30,000 incidents)
  - Most were unsuccessful attacks
- 69% reduction in successful attacks from Jan 2005 to Jan 2007
  - (from 130 successful attacks to 40)
- 61% reduction in DoD computers used in BOTNETs from Feb 2005 to Jan 2006
  - Machines in BOTNETs in the Internet increased by roughly 110% in the same period
- Adversary behavior is changing owing to tightening of systems
  - 5,267% increase in socially engineered email attacks from January 2006 to September 2006
  - 62% decrease from September 2006 to December 2006 owing to quick-reaction training DoD-wide, and reduction in web mail access

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 28, 2007

QUESTIONS SUBMITTED BY MR. SMITH

Mr. SMITH. What role do you play in transitioning IT efforts developed within the S&T community into the GIG?

Secretary GRIMES. The Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) monitors and supports a wide variety of Science and Technology (S&T) information technology efforts. Specific examples of NII/S&T community technology transition partnerships include: the Defense Advanced Research Projects Agency programs on advanced networking protocols; the Defense Venture Catalyst Initiative (DeVenCI); the Joint Concept Technology Development (JCTD) Programs; and the networking/information assurance research and development programs with the Director, Defense Research and Engineering. S&T efforts are transitioned into the Global Information Grid (GIG) by developing enabling integrated capabilities for the Joint Net-Centric Operations (JNO) Portfolio and GIG Systems Engineering Architecture.

Mr. SMITH. What is DOD doing in the realm of Information Assurance and how is this being managed as part of DOD's move towards net-centric operations?

Secretary GRIMES. To meet the rapidly changing needs of the warfighter and enable decision makers, our Information Assurance (IA) posture and net defenses are becoming stronger to provide a sufficient defense-in-depth in response to sophisticated nation-state adversaries which are well resourced, persistent and attack with precision. Our warfighters must have confidence in the networks that support them and be assured that the information they need is available when they need it, accurate, and has not been stolen or manipulated by our adversaries.

The DOD Chief Information Officer (CIO) IA transformational priorities focus on four key areas:

(1) Ensuring the Department's Global Information Grid is resilient and enables DOD Mission Assurance despite sophisticated attack;

(2) Restructuring the network design and operations to confine attacks to boundaries, improve reaction time to incidents and deny adversaries the opportunity to exploit weaknesses;

(3) Partnering with the Defense Industrial Base to collaboratively work towards safer and more secure ways of doing business; and

(4) Managing risk to our supply chain due to effects of globalization.

The DOD IA strategic plan and portfolio management processes approach security comprehensively and addresses people, processes, and technologies to ensure compliance with compliant with regulatory and statutory guidelines, policies and laws.

The Department's IA program proactively addresses the security challenges of the rapidly evolving threat by eliminating vulnerabilities through rigorous configuration and access control. For example, the Department has over 3.5 million personnel with common access card credentials to ensure robust identity management and access control to the networks. In addition, the CIO has instituted a comprehensive campaign to educate and train the DOD workforce on network vulnerabilities and it is in the process of certifying up to 90,000 personnel in Information Technology and Security skill fields.

Mr. SMITH. How does NII, in the oversight role, develop, coordinate, and implement cyber security and information assurance (IA) requirements development and implementation efforts across the DOD and Service IT portfolios?

Secretary GRIMES. DOD Instruction 8115.02, "Information Technology Portfolio Management (ITPM)", provides the mechanism that the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DOD Chief Information Officer (CIO) uses for making decisions and recommendations based on enterprise strategic planning, integrated architectures, and outcome-based performance measures to achieve the Global Information Grid (GIG) Information Assurance (IA) vision across the Department. The process:

- Ensures fully leveraged baseline of resources from research to decommission;
- Synchronizes project milestones and dependencies;

- Measures performance to drive and manage investment decisions;
- Recommends the best mix of investment; and
- Monitors the execution, ensure the results and take appropriate corrective actions on IA programs

Portfolio Management is integrated into DOD and Service Portfolios through the Joint Capabilities Integration Development System (JCIDS). JCIDS, is the formal DOD procedure defining acquisition requirements and evaluation criteria for future defense programs.

The IA Portfolio Management activities have been organized into six capability areas:

(1) Assured Information Sharing;
(2) Integrity/Non-Repudiation;
(3) Assured Mission Management;
(4) Defend the GIG;
(5) Highly Available Enterprise; and
(6) Confidentiality as defined in the approved JCIDS Joint Capabilities Document (JCD) and the GIG IA Initial Capabilities Document (ICD).

A DOD-wide IA Working Group (composed of representatives from each of the Combatant Commands Services and Agencies) is established to participate in lifecycle cost estimation, prioritization, and validation of all IA initiatives. In addition to addressing operational needs by selecting the best mix of investments, the Portfolio Management process reduces programmatic risk through a continued control and evaluation process. This provides insight into programs' and activities' cost, schedule, and performance to ensure that capabilities are being provided where and when they are needed. Portfolio Management also provides the ability to execute programmatic risk mitigations to adjust the portfolio and ensure that capabilities are delivered as planned.

Mr. SMITH. In the Milestone Decision process, what are the criteria for determining whether NII or Acquisition, Technology and Logistics (AT&L) holds Milestone Decision Authority (MDA) over programs? What programs have been claimed by both NII and AT&L for final MDA approval? How was the decision made to give MDA to one or the other organization?

Secretary GRIMES. The Under Secretary of Defense for Acquisition Technology and Logistics (USD(AT&L)) is the Defense Acquisition Executive and determines the Milestone Decision Authority (MDA) for DOD acquisition programs. Historically, the USD(AT&L) has delegated MDA for major automated information system (MAIS) acquisition programs to the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)). The USD(AT&L) retains MDA for major defense acquisition programs (MDAPs), except for those he elects to delegate to the Service Acquisition Executives. The primary reason for permitting the ASD(NII) to serve as MDA for MAIS has been that the expertise for MAIS programs is in the OASD(NII). In rare cases, when an MDAP is not a weapon system, and is primarily information technology (IT) oriented, the USD(AT&L) has delegated MDA to the ASD(NII).

The USD(AT&L) recently established an organization within OUSD(AT&L) with expertise in acquiring business systems. As a result, the USD(AT&L) has become the MDA for those business systems that are MAIS programs.

A few MAIS programs exceed the dollar threshold for an MDAP. When this happens, the program is classified as both a MAIS and an MDAP, often called a MAIS/MDAP. The USD(AT&L) determines who will serve as the MDA for a MAIS/MDAP.

No programs have been claimed by both USD(AT&L) and ASD(NII) for final MDA approval. All programs have only one MDA. However, when the USD(AT&L) is the MDA, the ASD(NII)/DOD Chief Information Officer has a key advisory role by serving as a member of the Defense Acquisition Board. When the ASD(NII) is the MDA, key members of the USD(AT&L)'s staff serve as members of the IT Acquisition Board.

Mr. SMITH. Can you explain to the subcommittee how you exercise your responsibilities under the Capability Portfolio Management (CPM) process for Joint Net-Centric Operations (JNO)? Do you believe that provides you will appropriate level of authority to manage these kinds of joint IT programs?

Secretary GRIMES. The responsibilities under the Capability Portfolio Management (CPM) process are met using three types of authorities provided to the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DOD CIO). The first type of authority is provided as the Principal Staff Assistant (PSA) to the Secretary of Defense for command and control (C2), communications, spectrum, information assurance, en-

terprise wide systems engineering, and related activities as enumerated in the NII charter. This set of authorities involves program oversight, establishing policies, and ensuring the requirements for the warfighter are being appropriately addressed in each of the PSA areas. The ASD(NII) PSA authorities clearly support the Joint Net-Centric Operations (JNO) CPM process and objectives.

The second type of authority vested with the ASD(NII)/DOD CIO is specified as the Department's CIO, specifically to ensure the IT investments are appropriate, as well as ensuring the systems are interoperable and the right level of information assurance is achieved. The DOD CIO authorities also directly support the JNO CPM portfolio since the JNO portfolio consists of enabling infrastructure components such as communication networks (transport), enterprise services, computing capabilities, information assurance, and network management components.

The third type of ASD(NII)/DOD CIO authority is specifically granted as the Capability Portfolio Manager of the JNO portfolio. The CPM process recommends and advises the owners of the three major department processes (capabilities, acquisition, and resources) relative to the specific portfolio functions. The CPM assesses and recommends actions regarding the execution and content of JNO (IT) programs to the Under Secretary of Defense for Acquisition, Technology and Logistics. The JNO CPM also addresses the capabilities issues with the Joint Staff J8 and Joint Requirements Oversight Council (JROC). Finally, the JNO CPM ensures the proper balance is maintained within the portfolio regarding the funding allocations and program investments using the 3-Star Programmers Resource Board and advising the Director of Program Analysis and Evaluation.

Mr. SMITH. Do you believe that provides you will [sic] appropriate level of authority to manage these kinds of joint IT programs?

Secretary GRIMES. Yes. The combined authorities of the ASD(NII)/DOD CIO as a PSA, the DOD CIO, and CPM offers the ability to influence, as well as execute, the objectives established for the JNO portfolio. In addition, the ASD(NII)/DOD CIO is lead chair for the Command and Control Capability Integration Board (C2CIB), which oversees all JNO and Joint C2 (JC2) portfolio activities. This board also acts as the fusion body for ensuring the JC2, JNO and Battlespace Awareness portfolios are appropriately addressing the joint needs. Also, the ASD(NII)/DOD CIO is a permanent member of the Deputy Advisory Working Group (DAWG), which oversees and directs all portfolio activities. Adequate authorities exist to achieve the management objectives for both Service specific and joint based IT programs.

Mr. SMITH. How do you suggest we move away from the traditional mindset of "need-to-know" and institutionalize systems based on "need-to-share"?

Secretary GRIMES. Changing the culture is a significant challenge and will take time. It requires increased awareness that all mission partners need each other to achieve optimal mission success (the warfighter on the battlefield understands this need). This culture shift must embrace improved sharing and collaboration capabilities as necessary to achieving operational goals. For DOD, these are closely related to the Secretary's Transformation Priorities, which include Building Partnership Capacity, Implementing the Cyberspace Strategy, and Homeland Defense/Civil Support Capabilities.

Implementing the "need to share" paradigm can be accommodated with information systems standards and capabilities developed concurrently and/or in conjunction with other Federal Agencies. Using venues such as the Federal Chief Information Officer Council or the Information Sharing Council to ensure that there is a common understanding of the importance of this new paradigm helps establish the mindset change needed at senior and staff levels across the government.

Mr. SMITH. How are DOD IT data and architectural standards coordinated with international and interagency partners (such as the Departments of State, Justice, Homeland Security and Treasury and the Intelligence Community)?

Secretary GRIMES. The Defense Information Systems Agency (DISA) is the Department of Defense (DOD) Executive Agent (EA) for Information Technology (IT) Standards, responsible for developing, publishing, and maintaining established and developmental interoperability standards. As the Department's EA, DISA identifies and assesses relevant emerging technologies and related standards; manages DOD participation in external IT standards developing organizations and standards setting organizations; facilitates feedback and dissemination of IT standards information among DOD stakeholders; and develops, acquires, adopts, specifies, maintains, and manages the life cycle of IT standards for DOD. DISA works closely with interagency partners to ensure that DOD's requirements are met with accredited standards that are available from or under development by authoritative non-government sources.

To accomplish this, DISA represents the DOD and participates in relevant external standards developing organization and standards setting organization activities

to ensure timely consideration of DOD requirements. For example, DISA recently worked with the National Institute of Standards and Technology (NIST) as well as the Department of Homeland Security (DHS) to arrive at federal consensus on the determination and suitability of an open document standard for International adoption. In addition, DISA is substantially involved with the government-wide Information Sharing Council to develop a pilot capability with the Department of Justice whereby DOD will be able to share DOD standards and metadata that pertain to Counter Terrorism Information Sharing and suspicious activity reporting with state, county, and tribal law enforcement entities.

With respect to international standards coordination, DOD must consider both its interests within NATO, as well as those of our Coalition partners and other non-NATO nations, on a bilateral basis. In many of these relationships, DOD expresses its position through its national representatives to the international standardization bodies such as the International Standardization Organization (ISO) and the Internet Engineering Task Force (IETF). In the NATO community, DOD participates in the NATO Command, Control, and Communications (C3) Board and various other NATO working committees principally involved in networked centric operations and tactical communications. In these environments, the Department is actively engaged in the management of U.S. military requirements in the form of NATO Standardization Agreements or STANAGs. Our non-NATO partners are usually interested in aligning to our Military and Commercial standards implementations to support their procurements of U.S. Military equipment via Foreign Military Sales. As an example, the coordination process within the NATO Joint Messaging Systems Working Group involves the development, evaluation and approval of change proposals that impact the platform implementation of tactical messaging STANAGs.

Additional information on DOD's IT standardization efforts can be found in the January/March 2007 issue of The Defense Standardization Program Journal, "DOD IT Standardization" at www.dsp.dla.mil/APP_UIL/content/newsletters/journal/DSPJ-01-07.pdf.

Mr. SMITH. What are you doing to manage and deconflict radio frequency spectrum issues at the tactical level (for example, to ameliorate the problem of IED jammers interfering with communications systems)? How do efforts like the Global Electromagnetic Spectrum Information System (GEMSIS); Defense Spectrum Management Architecture (DSMA) and the Defense Spectrum Office support operations at the tactical level?

Secretary GRIMES. The Department of Defense (DOD) has numerous efforts underway to manage and deconflict radio frequency spectrum at the tactical level. In the near term, DOD is actively addressing the problem of improvised explosive device (IED) jammers interfering with communications systems in theater by taking steps to minimize electromagnetic interference between our own forces. The near term investment calls for commercial-off-the-shelf (COTS) equipment combined with tactics, training and procedures (TTPs) to mitigate electromagnetic interference. This will be followed by programmatic solutions in the mid- and long-term to automate and sustain our new battlespace management capabilities.

The near-term efforts, which address a U.S. Central Command (CENTCOM) Joint Urgent Operational Needs Statement (JUONS), December 2005, include:

- Enhance electronic warfare analysis capability within the existing spectrum management tool (SPECTRUM XXI) and field it to the tactical level;
- Establish an Operational Spectrum Analysis Cell at the Defense Spectrum Organization (DSO) to provide 24-hour operational support to current operations in Iraq;
- Field portable spectrum analyzers in theater with supporting laptops; and
- Develop TTPs to address the electromagnetic spectrum interference.

In parallel, the Navy volunteered to provide over 200 Electronic Warfare Officers to assist with Counter RCIED (Remote Control Improvised Explosive Device) Electronic Warfare (CREW) jammer deconfliction. The Navy's addition has proved very valuable as the Army develops its own Electronic Warfare Officer career field.

In the mid-term, the DOD is developing the Coalition Joint Spectrum Management Planning Tool (CJSMPT) as a Joint Capabilities Technology Demonstration (JCTD), to mitigate CREW system and communications interference. The unique tool enables the warfighter to plan out, with modeling and simulation, the electromagnetic spectrum operating environment. Phase II will provide broader Joint Task Force level planning for spectrum access and deconfliction based on unit level spectrum requirements.

The CJSMPT will be mapped to the Global Electromagnetic Spectrum Information System (GEMSIS), as Increment I, using the Defense Spectrum Management Archi-

tecture (DSMA) to ensure the technology demonstration is sustained and kept current with the warfighter's needs. In the long term, GEMSIS will support evolving military operations and the Global War on Terrorism (GWOT) by transforming spectrum operations from a preplanned and static frequency assignment system into a responsive and agile capability to manage the complex electromagnetic spectrum battlespace. GEMSIS will provide a suite of tools that will enable planning at the strategic, operational and tactical levels. Battlespace management with GEMSIS will decrease operational risk significantly by reducing or eliminating electromagnetic spectrum interference, while enabling DOD to maximize our military investment through more informed procurement.

GEMSIS, as envisioned, will be built in line with the DSMA and leverage all existing spectrum management capabilities in its design. The DSMA provides the roadmap and transition strategy to evolve to DOD's spectrum management vision. Furthermore, it is used to ensure our efforts are synchronized.

GEMSIS will leverage work being conducted by the DSO, particularly the spectrum management data and tools transformation plans. These plans, worked in coordination with the entire spectrum community, will move us successfully into the future.

At the tactical level, as mentioned above, the DSO maintains the Operational Spectrum Analysis Cell at its Annapolis, MD facility, which provides technical support, deployable training teams and operational surge augmentation as needed to provide radio frequency support to ongoing military operations.

Mr. SMITH. Could you please update us on the status of the DOD Information Sharing Strategy, including when it might be completed and how it will impact DOD information policy?

Secretary GRIMES. The Assistant Secretary of Defense for Network and Information Integration/DOD Chief Information Officer (ASD(NII)/DOD CIO) anticipates signing the DOD Information Sharing Strategy in early May 2007. This Strategy will establish a new information sharing vision for the Department of Defense: "Delivering the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment."

The DOD CIO is working closely with the President's Information Sharing Environment Program Manager and the Associate Director of National Intelligence and Chief Information Officer to ensure that DOD goals address the broader National Strategy for Information Sharing.

To make immediate progress in achieving the goals of the DOD Information Strategy, a companion Implementation Plan is being developed. This Plan will outline near-term tasks and offices of primary responsibility that impact the full spectrum of information sharing concerns. Chief among these concerns is ensuring that effective policies are in place to enable information sharing. Accordingly, task considerations in the Plan include the development of overarching information sharing Directive as well as making improvements in existing policies dealing with classification and release processes. The Implementation Plan is scheduled to be signed in the second quarter of FY08.

Mr. SMITH. What is DOD's role in the Information Sharing Environment (ISE) program called for in the Intelligence Reform and Terrorism Prevention Act? What is the status of ISE?

Secretary GRIMES. DOD is actively involved in Information Sharing Environment (ISE) activities through the Information Sharing Council and working groups reporting to the ISC.

DOD provides leadership via the ISC in order to centrally describe the ISE missions and processes while relying on an implementation approach based on a distributed, federated model. An example is the implementation of the Controlled Unclassified Information (CUI) framework. The CUI framework implements a new marking, safeguarding, and dissemination scheme. With the PM ISE lead in identifying and defining ISE-level CUI implementation activities, e.g., establishing governance rules for dissemination until the CUI executive agent is identified, DOD is developing plans to identify needed DOD CUI policy and scope—one that extends to all forms of DOD information while addressing information sharing with external partners. Similarly, DOD is establishing procedures to review existing DOD Sensitive But Unclassified information to determine priorities, mechanisms, and time frames for re-marking information that is reused in the CUI environment.

Mr. SMITH. What is the status of ISE?

Secretary GRIMES. The ISE Implementation Plan was completed in November 2006 and describes six goals to be achieved over the next three years:

- Facilitate the establishment of a trusted partnership among all levels of government, the private sector, and foreign partners.

- Promote an information sharing culture among ISE partners by facilitating the improved sharing of timely, validated, protected, and actionable terrorism information supported by extensive education, training, and awareness programs for ISE participants.
- To the maximum extent possible, function in a decentralized, distributed, and coordinated manner.
- Develop and deploy incrementally, leveraging existing information sharing capabilities while also creating new core functions and services.
- Enable the Federal government to speak with one voice on terrorism-related matters, and to promote more rapid and effective interchange and coordination among Federal departments and agencies and state, local, and tribal governments, the private sector, and foreign partners, thus ensuring effective multi-directional sharing of information.
- Ensure sharing procedures and policies protect information privacy and civil liberties.

The PM ISE first report to Congress will be issued in September 2007 and will describe the activities accomplished since the inception of this office.

The PM ISE anticipates releasing the National Strategy for Information Sharing in October 2007. The Strategy will provide a framework for enhanced information sharing among Federal, State, local, and tribal officials, the private sector, and foreign partners to aid their individual missions and to help secure the homeland. It will also describe the Federal Government's approach to support State and major urban area fusion centers. The Strategy will also continue to ensure that privacy and civil liberties of Americans are safeguarded.

Mr. SMITH. What steps has DISA taken to evaluate the vulnerabilities and threats that potentially affect the DOD's communications infrastructure? What plans and programs do you have that are addressing these vulnerabilities? How will DISA be flexible in the future to address vulnerabilities and threats to our networks in the future?

General CROOM. DISA, its partner the Joint Task Force for Global Network Operations (JTF GNO), and the Department of Defense have a wide variety processes and programs to ensure that DISA, the JTF GNO, and other DOD components are aware of, and respond to the vulnerabilities and threats that potentially affect the DOD's communication infrastructure.

DOD tracks and learns of vulnerabilities in the information technologies used by the department in a variety of ways. The first is that the JTF GNO monitors commercial vulnerability research and alerting services. These keep us up-to-date with what is known by researchers and by industry about vulnerabilities in specific products and technologies. A second method is to do careful analysis of attacks against federal government computers to determine whether the attacks exploit a vulnerability not known via other vulnerability research processes.

A third approach is done as a core part of the DOD's certification and accreditation process, which is the process for ensuring that security is properly considered in the design, deployment, and operation of systems. During the certification and accreditation of a particular product or system, the DOD performs a security analysis, which may uncover vulnerabilities. The depth of the analysis varies depending on the criticality of the system and on whether other factors of the system's environment might reduce certain types of risks. This sort of analysis is repeated regularly during a system's lifetime, with the repetition rate depending on the criticality of the system and on whether other vulnerability processes provide new information that indicates a review is warranted.

The DOD also regularly tests the cyber security of its operational systems and of the processes associated with the security of these systems. An example is the DISA enhanced compliance validation visit process. DISA has teams that are under the operational control of the JTF GNO that visit selected government sites that are connected to the core DOD networks (the unclassified network, called the NIPRNET, and the Secret network, called the SIPRNET). These teams examine the policies and procedures at the site, and perform tests and checks to determine the site's compliance with the department's cyber security standards. Another example is the information assurance evaluation that the Joint Interoperability Test Command performs during certain military exercises.

The JTF GNO has an active intelligence analysis organization that teams with partners throughout the intelligence community to analyze the threat to DOD networks. The information derived this way is combined with information about attacks and incidents in the federal government and elsewhere, with information about the vulnerability of particular technologies, and with information about the design of

DOD systems to develop operational, programmatic, and budget plans and priorities.

Certification and accreditation. As a first step, DISA and the JTF GNO work to ensure the core process of certification and accreditation is working properly and is applied to every system on which DOD depends. DISA and the JTF GNO are also participating in an effort among the DNI, the DOD, the National Institute of Standards and Technology (NIST), and others to improve the certification and accreditation process throughout the federal government. DISA and the JTF GNO also participate in the DOD-wide community risk management processes that consider the mission risk and the mission benefit of deploying certain systems or technologies that are used broadly in the DOD or that have risk implications across a large subset of the Department. This latter process starts with the Defense Information Systems Network (the DISN) Security Accreditation Working Group (the DSAWG) that DISA chairs. The group has participants from throughout the Department and from the intelligence community. The DSAWG makes recommendations to a higher level group called the DISN flag panel, which ultimately makes decisions about whether to deploy the system under consideration, and makes decisions about the revisit rate for security evaluation and re-approval.

Configuration and other security guidance. A second program for addressing the vulnerabilities is the effort to define the appropriate security controls for DOD systems, then to define the proper (the secure) configuration for technologies and products used in the system. DISA has partnered for years with NIST, with NSA, and with industry to produce guidance on how to properly configure operating systems and key applications so that vulnerability is reduced or eliminated. NIST, NSA, and DISA produce portions of the overall set of these guides, and we are all working to move more of the work to our industry partners (since as the product developer, a particular vendor is in the best position to understand how to configure the product securely). These guidance documents are updated regularly as new information about vulnerability and threat becomes available, and as the technologies change. DISA and the JTF GNO are also participating in the effort being led by NIST to develop a broad set of data standards so that the processes of configuring a system securely, the process of measuring the configuration automatically and regularly, and the process of understanding and responding to an attack can become more automated. The NIST-led effort is called the Security Content Automation Protocol (SCAP). DISA is moving to ensure that the DISA-developed configuration guides are published in SCAP-conformant form, and that other tools we deploy are capable of consuming and producing information in SCAP format.

Vulnerability alerting and mandated configuration changes. Ensuring that DOD information systems and enclaves are properly configured is essential. In addition to the definition of the security standards above, the JTF GNO operates processes to monitor the various sources of vulnerability information and to alert DOD to new vulnerabilities, and to direct changes to system configurations as the new information and the JTF GNO's analyses indicate. This process is called the Information Assurance Vulnerability Alert (IAVA) process. Since the JTF GNO is the top operational entity in the DOD's networks, all subordinate organizations must acknowledge receipt of an alert, and must also regularly report compliance with the mandated action.

Attack detection, diagnosis, and reaction, including communication tasking orders. The JTF GNO, along with the other network operations entities of the Department monitors the Department's networks for intrusion, attack, and attempted attack. They use a system of DOD-developed, and commercial detection and analysis systems. In response to an attack or an incident, the JTF GNO may direct that a number of different actions be performed, from further analysis of the incident, to "cleaning" of the affected systems, to changing the protection settings of core protections of the department. In a process that is closely related to the IAVA process, the JTF GNO issues another type of order to all network operations entities in the Department. This type of order is called a Communications Tasking Order (CTO) and is issued whenever, in the judgment of the JTF GNO, a change in the way DOD operates and protects its systems is indicated. An example of an action directed by a JTF GNO CTO is a change in the protection settings at the boundary between DOD and the Internet. When doing this, the JTF GNO considers the end-to-end design of the DOD networks, and when necessary, changes the outer-boundary protections via a CTO issued to everyone who operates a connection between DOD and others. Another example is the mandate for all DOD entities to log into the DOD networks using a DOD Public Key Infrastructure (PKI) credential. The PKI logon CTO was issued in response to an increase in attempts, both unsuccessful and successful, to exploit the vulnerabilities of plain text passwords in DOD networks.

Management of the DOD information assurance portfolio. DISA and the JTF GNO participate in a process sponsored by the Assistant Secretary of Defense for Networks and Information Integration called the Global Information Grid (GIG) Information Assurance Portfolio (GIAP) management process. The GIAP office is staffed primarily by the National Security Agency, although the deputy GIAP manager is from DISA. The GIAP process is focused on ensuring that the DOD information system security program is focused on the right mix of near-term and longer term protections and processes for the networks of the department and of the federal government. It does this by looking at vulnerabilities, threat, current efforts, technology changes, etc. DISA and the JTF GNO provide input throughout the GIAP resource prioritization process. These range from providing data on current programs, to providing inputs and participating in design studies, to providing inputs on current operational priorities, to helping to explain the program in various higher-level DOD resource allocation fora. The JTF GNO also produces operational requirement documents focused on places the JTF GNO considers program priorities.

A large piece of the overall Global Information Grid IA portfolio is overseen by the Computer Networks Defense Enterprise Solutions Steering Group (the CND ESSG). This group is made up of representatives from the military services, U.S. Strategic Command, the JTF GNO, NSA, and DISA. The group meets roughly quarterly for several days and reviews data on current programs, changes in the threat, changes in DOD's vulnerability posture, changes in technology, and then determines what (if any) changes should be made to the portion of the GIAP that it oversees. The JTF GNO serves as the requirements lead for the CND ESSG. DISA acts as the program manager for the ESSG and is responsible for acquiring, helping to pilot, and then supporting the deployment of computer network defense tools and technologies used DOD-wide. A few examples of these tools include a configuration scanner/vulnerability scanner, antivirus scanners, and an automated configuration change tool.

Within the portion of the information assurance portfolio that is DISA's responsibility, DISA regularly examines efforts that are either underway or planned in order to ensure they are still focused on the appropriate priorities and are still countering the threat against the vulnerabilities in DOD networks as we understand them at that moment.

Ports and protocols process. In addition to chairing the DSAWG, and operating the network compliance validation teams, DISA operates another core risk management process for the department. The ports and protocols process is focused on ensuring that the different layers of network perimeter defense in the Department properly balance interoperability of joint applications, with security.

DISA information assurance program. DISA has a wide variety of efforts focused on protecting the networks of the Department, and focused on detecting, diagnosing, and reacting to attacks when the protections are insufficient. These efforts are focused on several broad areas of information assurance. One is hardening the end computer (whether a server or workstation) by defining the secure configuration, then helping to automate the configuration and measurement processes, and by acquiring and deploying additional hardening tools (e.g., antivirus scanners). Another area is ensuring the perimeter defenses deployed by DOD operators are properly placed and configured to best support interoperability and security. A third area is ensuring that applications are designed in a secure way, and in a way that ensures the application operates properly on a secured computer, and with the different layers of perimeter defense.

Another area is that of eliminating inappropriate anonymity in the networks by providing a non-replayable cyber identity credential and enabling its use in more and more interactions within the Department and external to it. The DOD public key infrastructure program, and related directory and application guidance efforts are the primary components of this area. A fifth area is the design, deployment, and operation of an infrastructure to detect and diagnosis attacks sufficiently well that network operations entities can rapidly construct militarily useful courses of action, then execute the most promising. In addition to this infrastructure, the DISA Theater NETOPS Centers (TNCs), working under the JTF GNO, provide an attack detection and diagnosis service to the Combatant Commanders, and certain others in the Department. DISA also builds systems that collect the data about compliance (with vulnerability standards, with CTOs, with IAVAs, etc.) and that provide readiness and vulnerability information to both operational and programmatic decision makers.

Information assurance in information technology efforts that DISA manages. The certification and accreditation process, the DISA system engineering process, and the DOD acquisition process all combine to ensure that in each area in

which DISA is responsible for deploying and/or operating information technology, (for instance command and control, the network, enterprise computing), the effort has appropriate information assurance.

DOD-wide IA training. DISA develops and distributes core information assurance training material for the Department. These courses are continuously updated to reflect the latest vulnerabilities, threats, technologies, DOD trends, and the like.

All of the processes and efforts described above are aimed at ensuring that DISA's efforts, the JTF GNO's efforts, and DOD's efforts keep pace with changes in vulnerability and threat. In addition to these, DISA tracks and leads the deployment of certain technologies in the Department, and also uses this information in constructing the product mix in its information assurance efforts. The following are two examples of what DISA is doing to consider changes in technology in DISA's ever evolving information assurance efforts.

DISA is advocating, along with others, a movement to the SOA style of building applications and business processes in the Department. This is how the new joint command and control capability, called Net-Enabled Command Capability (NECC) will be constructed. The SOA means that different DOD and non-DOD entities will provide services that are available on the network, and that an application developer will "compose" an application from these network-based services. This will be a significant change in the security model for applications, and so, as part of the Netcentric Enterprise Services Program, DISA is providing guidance documents that describe the security services (and other standards) needed at the service interface, including the standards for a new form of access control called attributed-based access control. DISA is also providing source code samples for these interfaces, and is providing a Joint Enterprise Directory Service to enable this new form of access control.

DISA, via its Chief Technology Officer, operates a technology reconnaissance office that helps DISA recognize and stay in front of information technology trends, whether from industry or academia. The output of this effort is used as input to the DISA and to the GIAP information assurance definition and prioritization processes.

Mr. SMITH. The Joint Interoperability Test Center has been given a recent mandate to create a test and evaluation methodology to accelerate delivery of Service Oriented Architecture based information processing capabilities. Could you explain what you mean by "service-oriented architecture" and why this is an important departure from how we have done business in the past? What is JITC's status in developing this T&E methodology?

General CROOM. Service-oriented architecture (SOA) is an approach for enabling information sharing across complex information technology (IT) systems that is rapidly being adopted in both the public and private sectors. At the most fundamental level, SOA is a way for many and diverse stakeholders to share information and perform IT functions for others over a network. These functions, or services, are provided using well defined interfaces to avoid unnecessary dependencies among stakeholders' systems. By enabling the sharing of functions across traditional system boundaries, stakeholders need not build systems themselves for every function to be performed.

Operating in a SOA, there are two important stakeholders, the provider or the one who performs the function, and the consumer or the one who requests the function be performed. Prospective consumers can discover available services and choose to have providers provide services to them. Providers offer to perform services and do not necessarily need to know in advance who the consumers may be. The interaction of the provider and consumer occurs through a service interface described by a service agreement between the two stakeholders. The service agreement can define requirements and objectives such as intended use, performance guarantees, and information assurance requirements.

Mr. SMITH. Could you explain what you mean by "service-oriented architecture" and why this is an important departure from how we have done business in the past?

General CROOM. The service-centric approach of SOA is fundamentally different than the system-centric approach that has been used in the past. Rather than focusing on the development of monolithic systems based on fixed requirements and single user communities, SOA focuses on rapidly evolving services that can be consumed by others to support changing mission needs. Effective use of SOA leads to reduced redundancy and improved flexibility, effectiveness, and efficiencies. SOA also enables stakeholders to implement and evolve their IT environments independently. Providers have greater capability to modify, extend and rapidly improve individual services independently, and consumers have the ability to implement new or altered business processes at a level that is largely independent of any particular

IT system. This flexibility coupled with consumer choice, enables the agility necessary to rapidly respond to changing needs and threats. Benefits of SOA include:

- **Interoperability:** Ability to seamlessly share functions capabilities and information across organizational boundaries regardless of their underlining technology, platform or location.
- **Agility:** Ability to dynamically reconfigure processes to meet changing operational requirements. SOA reduces integration costs and makes the enterprise more adaptable to dynamically changing mission needs and operational situations. These improvements facilitate the warfighter ability to adapt and respond inside the enemy's decision loop.
- **New and Enhanced Capabilities:** Since a consumer can choose from a range of services offered over the network rather then just those functions supported offered within their own systems, new capabilities can be rapidly enabled.
- **Visibility:** Common understanding of requirements and capabilities among consumers, planners and providers enabling the justification of IT investments on a basis of clear return on investment and seamless alignment of IT investments with mission requirements.

Mr. SMITH. What is JITC's status in developing this T&E methodology?

General CROOM. The Joint Interoperability Test Command (JITC) has developed methods for testing SOA-based capabilities to ensure the warfighters' operational needs are effectively met. The elements outlined below provide the foundation for interoperability test methodology for SOA-based capabilities.

- **Standards.** Test methodology to assess compliance to standards important to net-centric operations
  - Verify capabilities meet DOD implementation guidance for connecting to the GIG.
  - Verify capabilities meet DOD implementation guidance for use of net-centric standards, e.g., SOAP, WSDL and UDDI.
- **Data and Services.** Test methodology to verify data and services are visible, accessible, and understandable
  - Data and services are discoverable and available at an enterprise level, e.g., registered in enterprise level repository/catalog, and support service level agreements
  - Guidance is published and used for gaining access to data/services, e.g., electronic identification, authentication, and authorization
  - Data can be used as information that supports mission requirements
- **Information Assurance (IA).** Test methodology assesses compliance that services are trusted and secure.
  - Verification the system/service meets requirements for integration into an operational environment by reviewing DOD IA Certification and Accreditation Process (DIACAP) documentation
  - Validation that the system/service is configured in accordance with approved security guidance using scans, gold disks, and display of enclave device settings
- **End to End Operational Effectiveness.** Ensures capability enhances mission effectiveness
  - Testing using mission threads in relevant and operationally realistic environments.

JITC is executing and refining this methodology through a series of pilot efforts specifically supporting enhanced capability for command and control using the Net-Enabled Command Capability program.

QUESTIONS SUBMITTED BY MR. THORNBERRY

Mr. THORNBERRY. You have responsibility for Department of Defense Networks and Information. Who has responsibility for the non-DOD/IC government networks?

Secretary GRIMES. The non-DOD/IC government networks come under the purview of the Director, National Intelligence (DNI) CIO who in turn interfaces extensively with the CIOs for the agencies within the IC. The other non-DOD related networks are under the purview of the Department of Homeland Security (DHS) CIO.

DOD CIO works closely with the DNI CIO and also has a good working relationship with the DHS CIO.

Mr. THORNBERRY. Who has responsibility for the commercial networks or "backbones"?

Secretary GRIMES. Within the United States, the commercial networks are administratively governed by the Federal Communications Commission and Federal Trade Commission. The National Communications System, which is part of the Department of Homeland Security, synchronizes the activity of commercial carriers in support of government operational needs. The Department of Defense has long haul communications requirements worldwide that are supported through multiple contracts with commercial carriers, both foreign and domestic. The Department mitigates risk and dependence by maintaining control of the switching fabric and deriving connectivity from a diversity of carriers; thus allowing the Department to reroute its networks in the event of an individual carrier failing. This strategy includes both terrestrial and satellite networks.

Mr. THORNBERRY. You mentioned attacks on the DOD IT Infrastructure and protecting against that. Is it still true that about 90% of the DOD IT Infrastructure rides on the relatively unprotected commercial backbone?

Secretary GRIMES. The DOD Global Information Grid (GIG) includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. As Lt. Gen. Croom stated during the hearing on March 28th, the DOD military network includes 120,000 leased circuits and commercial satellite communications. The majority of the DOD IT Infrastructure leverages the commercial backbone to reach approximately 3,940 Base/Post/Camps/Stations in over 88 nations. The DOD GIG is global, mobile, and interconnected. Our dependence on a shared critical information infrastructure is our strategic advantage as well as our weakness.

Mr. THORNBERRY. What happens if there is a catastrophic attack against the commercial infrastructure that also brings down the DOD communications?

Secretary GRIMES. The Federal Government has a primary role in responding to cyber threats and assisting in recovery from and remediation of cyber incidents requiring a coordinated Federal response. The National Cyber Response Coordination Group (NCRCG), of which DOD is a co-chair (with the Department of Homeland Security and the Department of Justice) provides a mechanism for ensuring that sound, strategic decision-making accompanies the Federal Government's management of a cyber incident. DOD communications ride on commercial infrastructure which is why the Department is working to ensure redundancy and resiliency in the architecture and to ensure operators are knowledgeable and trained on work arounds. While there are limited fallback capabilities, the DOD has taken additional steps to increase resilience against sophisticated cyber attacks including the formation of a working group that was charged with analyzing the issue and laying out a plan of action to ensure the Department of Defense is able to accomplish its critical missions when networks, services, or information are unavailable, degraded, or untrusted. The interest in and concern about network security is increasing in the National Security and Emergency Preparedness (NS/EP) Communications, Intelligence, and Defense communities, as well as in agencies across the Federal Government. The Department is working with the President's National Security Telecommunications Advisory Committee's (NSTAC) Global Infrastructure Resiliency Task Force (GIRTF) and Network Security Scoping Group (NSSG.)

Mr. THORNBERRY. Who is responsible for finding the origin of the attacks and restoring the network; and how is it managed?

Secretary GRIMES. With respect to attribution, it is a difficult topic in cyberspace. The Intelligence community plays a key role in improving intelligence capabilities in cyberspace to facilitate attribution. Our ability to leverage the full spectrum of intelligence to support cyberspace operations is essential for situational awareness and response options to deal with an asymmetric and pervasive cyber threat. As stated above, the Department of Defense is a co-chair, with the Department of Homeland Security and the Department of Justice, of the National Cyber Response Coordination Group (NCRCG). The NCRCG is comprised of subject matter experts from Federal agencies who have roles and responsibilities related to investigating, defending against, responding to, mitigating, and assisting in the recovery from a Cyber Incident. When a cyber incident occurs, the Secretary of Homeland Security takes on the role as Principal Federal Official for incident management under HSPD 5. For restoring the network this depends where network was attacked, either the backbone provider, the ISP, or the local network owner would be responsible for restoring their portion of the network.

Mr. THORNBERRY. How does DOD respond?

Secretary GRIMES. Within DOD, the United States Strategic Command (USSTRATCOM) has been designated as the military lead for defending the DOD Global Information Grid (GIG). USSTRATCOM has responsibility for coordinating, supporting, and conducting computer network operations (CNO) in support of regional and national objectives. Through the Joint Task Force-Global Network Operations (JTF-GNO), USSTRATCOM directs the operation and defense of the GIG to assure timely and secure net-centric capabilities in support of DOD's full spectrum of warfighting, intelligence, and business missions. In its execution of cyber defense missions, the DOD employs a defense-in-depth approach and each of the Services and other Combatant Commands implement complementary policies, structures, roles, and missions. For security reasons, we do not discuss specifics about how this mission is carried out.

In the event of a cyber incident, the National Cyber Response Coordination Group is convened to develop courses of action and incident response strategies for the Federal Government, and the DOD, as co-chair, participates accordingly.

Mr. THORNBERRY. How does the rest of the federal government respond?

Secretary GRIMES. The Department of Homeland Security (DHS) has the responsibility of assuring the security, resiliency and reliability of the Nation's information technology and communications infrastructures. The DOD is responsible for defending the DOD Global Information Grid, but in regards to homeland security and cyberspace issues, DHS has the lead for the federal government.

Officials from DHS, Department of Justice, and Department of Defense serve as co-chairs for the National Cyber Response Coordination Group (NCRCG). Approximately 17 Federal departments, agencies, and entities with a role in cyber security, cybercrime, or protection of the critical infrastructure/key resources (CI/KR) have a role in the NCRCG.

Mr. THORNBERRY. Do you see any changes in authorities and policies to ensure DOD is able to operate and protect the network, particularly in the area of active defense?

Secretary GRIMES. A number of Departmental policies delineate roles and responsibilities in operating and defending the DOD's Global Information Grid. While active defense introduces a potentially new operational dimension through its machine-to-machine characteristics and its potential to instantly impact adversarial networks and cyberspace, it does not, by itself, necessitate the creation of new policy.

In terms of traditional information assurance and computer network defense, the DOD is guided by some 60 policy documents that range from directives and instructions to policy memorandums and technical bulletins. The authorities are largely established by law, organizational missions, and/or mission planning processes, and generally rest on the idea that distributed approval authorities are responsible for the security and stewardship of their individual enclave. Combatant commanders, military services, defense agencies and field activities conduct defensive network activities based on local requirements, centralized direction and established standards. This is no reason to suspect these policies or approaches are inappropriate or inadequate.

Where active defense is concerned, response actions are automated and reaction times are significantly condensed, thus potentially eliminating human discretion in the application of defensive triggers and cyber effects. This presents possible new legal frontiers in future iterations/applications of active defense, as policy-based programming will require the establishment of computer rules that potentially transcend U.S. Code and agency jurisdiction (e.g., Justice, DHS, Intelligence). This paradigm, however, is not arguably different than what exists today.

Although active defense does not yet warrant the creation of new network defense policies, legal considerations should be socialized and captured as we begin to institute automated defense capabilities on a more widespread basis.

Mr. THORNBERRY. Is taking the cyber fight offshore, to the adversary, considered an act of war by the foreign country receiving this military cyber action?

Secretary GRIMES. [The information referred to is classified and retained in the committee files.]

Mr. THORNBERRY. How does DOD consider the War Powers Act in terms of cyber warfare?

Secretary GRIMES. [The information referred to is classified and retained in the committee files.]

Mr. THORNBERRY. Given many of the cyber intrusions/attacks the USG sees today are often hidden through U.S. Internet sites, how will DOD coordinate their strike actions with U.S. law enforcement or homeland security authorities?

Secretary GRIMES. The span of DOD defensive response actions and the amount of coordination with U.S. Law Enforcement/Homeland Security Authorities is based

upon both the parties affected and the severity of the intrusion/attack. In most cases, responses to the intrusions/attacks are in line with those procedures and processes normally associated with incident handling and information sharing. In recent years, DOD has made dramatic improvements in its coordination with and in the sharing of information with U.S. Law Enforcement/Homeland Security. This has enabled an increased responsiveness on the parts of both DOD and U.S. Law Enforcement/Homeland Security while simultaneously maintaining the appropriate safeguards and policies that govern our respective responsibilities. For those cases where an active response may be warranted, guidelines and procedures have been established that provide for the coordination of actions based on both National and DOD Cyber Operations related directives and plans. United States Strategic Command (USSTRATCOM) Joint Task Force-Global Network Operations (JTF-GNO), regularly participates in the Department of Homeland Security/Department of Defense/Department of Justice led National Cyber Response Coordination Group (NCRCG). In an attack on DOD networks, all DOD parties adhere to the Secretary of Defense's (SECDEF's) Standing Rules of Engagement/Standing Rules for the Use of Force for Information Operations. For network attacks on U.S. Civilian Infrastructure, DOD participation in a U.S. Law Enforcement/Homeland Security led active response action would be governed by the existing laws concerning DOD/Military Support to Civil Authorities or as assigned and authorized by SECDEF. In all cases, military actions within the U.S. are a measure of last resort.

Mr. THORNBERRY. How do the Services, the operational commanders, and the Intelligence Community coordinate their activities?

Secretary GRIMES. The most mature process for coordinating United States Strategic Command's (USSTRATCOM's) Joint Functional Component Command of Network Warfare (JFCC-NW) offensive cyber operations with the Services, the operational commanders, and Intelligence Community is a JFCC-NW led joint interagency group of over 25 participants supporting the Global War on Terrorism. Additionally, while this forum primarily focuses on offensive cyber operations, it serves as an excellent model for future integrated offensive and defensive cyber operations of the United States Government.

Today, the National Cyber Investigative Joint Task Force (NCIJTF) coordinates DOD, Intelligence Community, and Law Enforcement/Counter-Intelligence Community efforts concerning network intrusions and attacks from Law Enforcement/Counter-Intelligence framework.

Currently, the National Cyber Response Coordination Group (NCRCG), led by a tri-chair from Department of Homeland Security, Department of Defense, Department of Justice, and consisting of representatives from most of the major Federal Departments, synchronizes and coordinates the Federal Government's National Cyber Defensive efforts.

Mr. THORNBERRY. Are we doing anything to adopt private industry's practices of remotely provisioning the network with patches, or are we relying on people to comply with JAVAs? Are there enough trained personnel to manually patch each vulnerability? What are we doing to enforce compliance with IAVAs and configuration guidance?

Secretary GRIMES. *Are we doing anything to adopt private industry's practices of remotely provisioning the network with patches, or are we relying on people to comply with IAVAs?*

The Department of Defense (DOD) does embrace the industry approach of remotely provisioning systems and network security patches as a best practice, through the centrally funded provision of automated scanning and remediation tools, SCCVI and SCRI,[1] and supporting policies and instruction. These tools have been provided for use by Information Assurance and system administration staff of all DOD Combatant Commanders, Services, Agencies and Functional Areas (CC/S/A/FAs) since November 7th 2005; automated scanning and remediation has been mandated since February 28th 2006.[2]

No viable solution exists to deliver software patches, remotely, to all systems in a heterogeneous network of the size and complexity of the GIG. For this reason DOD relies on the Information Assurance and network administration staff of CC/S/A/FAs to comply with the Information Assurance Vulnerability Management (IAVM) program specified at CJCSM 6510.01 Change 2, by detecting vulnerabilities and applying software patches identified in Information Assurance Vulnerability Alert (IAVA) notices using automated vulnerability scanning and remediation tools, wherever possible.

---

[1] Secure Configuration Compliance Verification Initiative (SCCVI) and Secure Configuration Remediation Initiative (SCRI).

[2] From Communication Tasking Order 05–19 dated November 7th 2005.

However, our tools, policies and procedures are reviewed frequently and significant DOD effort is being invested in the study and adoption of a Data Standards framework. For vulnerability management, National Institute of Standards and Technology's (NIST's) SCAP (Security Content Automation Protocol) standards will provide a framework for mapping operating systems and applications to vulnerabilities and patches, enabling more capable automated scanning and remediation tools in the future.

Are there enough trained personnel to manually patch each vulnerability?

With the availability of automated tools, there is no requirement to manually patch each vulnerability; however, automated solutions do not yet work for all platforms, requiring some manual patching. IAVM program compliance results suggest that, even with the best-of-breed automated tools that exist today (which ease some of the burden of patching), adequately staffing DOD's network management requirements is a challenge.

The Department employs various methods to deliver information security training to its technical workforce, and user awareness training to its worldwide workforce. These include traditional classroom training at Service schools and the private sector, professional military education courses, Service academies, and graduate schools; computer-aided instruction and web-based training; and multiple information security products and activities. DOD policy 8570.01-M "Information Assurance Workforce Improvement Program" defines personnel with significant information assurance (IA) responsibilities as those individuals performing Designated Approval Authority (DAA), Information Assurance Manager (IAM), and/or Information Assurance Technical (IAT) functions. This manual leverages industry best practices and raises the bar on commercial IA certifications by requiring they be accredited to an ISO standard for organizations that certify people.

As reported in the FY07 DOD FISMA report, the IA Workforce Improvement Program accomplishments for FY 2007 include:

- Expanded the number of universities designated as Centers of Academic Excellence in IA Education to 86 in FY 2007. These include 4 DOD schools (U.S. Military Academy, U.S. Air Force Academy, Air Force Institute of Technology, and Naval Postgraduate School).
- Continued aggressive use of the DOD IA Scholarship Program: 42 students graduated in 2007, 62 students awarded scholarships in 2007, 289 students have participated since the program's inception in FY01, and 179 students have graduated since the program's inception.
- Met its initial year implementation goal to certify (using commercial IT security certifications) 10% of the IA workforce.

What are we doing to enforce compliance with IAVAs and configuration guidance?

Secure system configuration is directed and mandated through the JTF-GNO managed IAVM program and through the Defense Information System Agency (DISA) Field Security Operations (FSO) team that produces Security Technical Implementation Guides (STIGs) for critical IT products, covering a variety of Operating Systems, applications, databases, networked services and network infrastructure. Another DISA-developed product, the 'Gold Disk', has been developed for some OS versions to help System Administrators determine the configuration of a computer and automatically fix most configuration vulnerabilities in line with the STIG guidance. The Federal Desktop Core Configuration (FDCC) standard also provides a baseline secure configuration, and has been incorporated into STIGs.

JTF-GNO tracks the response of CC/S/A/FAs to every IAVA that is issued under the IAVM program IAW CJCSM 6510.01 Change 2. Poor response is monitored and reported to the Commander, JTF-GNO each quarter, and routine engagement with CC/S/A/FAs through the Action Officer, DCDR and CDR is increased whilst outstanding issues are resolved. This process is under review by JTF-GNO, in concert with OSD(NII).

The DOD also regularly validates the cyber security of its operational systems and of the processes associated with the security of these systems. An example is the DISA Enhanced Compliance Validation (ECV) visit process. DISA has teams that are under the operational control of the JTF-GNO; these teams visit selected government sites that are connected to the core DOD networks (the unclassified network, called the NIPRNET, and the Secret network, called the SIPRNET). Each ECV team examines the policies and procedures at the site, and performs tests and checks to determine the site's compliance with the department's cyber security standards. The findings are back-briefed to JTF-GNO leadership who monitor any required remediation action to closure. Lessons-learned are captured and shared across the DOD IA community to aid in local self-assessment efforts, stimulate pol-

icy and technical guidance review, and inform future engineering and training efforts.

Mr. THORNBERRY. It has been widely reported that GEN Cartwright has characterized the current information operations structure as "dysfunctional." What is your view and what can we do to help?

General CROOM. While I would agree that the structure we work within today isn't perfect, I think General Cartwright's comments are founded on the idea that current laws and regulations present some organizational difficulties that prevent us from yielding capabilities as quickly as we would like.

Whether we call it Information Operations (IO) or cyberspace, the terms demand that we bring together a wide body of formerly disparate players into a relatively new mission set. For the DOD, this means electronic warfare specialists as well as computer network operators and even special operations forces must now be cognizant of how their once-isolated missions now affect the greater landscape of cyberspace. The Department has a strong doctrine and a number of Department-wide venues that attempt to mold this new space and deconflict roles and responsibilities. As with any transformational effort, there's a good deal of work to go in refining the mechanics and synchronizing policy, but I think we're enjoying healthy debate while moving the culture in the right direction.

At the National level, cyberspace security crosses many U.S. Codes—from Title 10, Title 50, Title 44, Title 18 and Title 6—and hence the resulting structure is composed of agencies and organizations who've never had to jointly confront the kinds of threats that we face today. We have seen very promising success from pilot efforts that literally bring the interagency players together to confront our adversaries in cyberspace, and in that regard I think we are well on our way to gaining understanding, resolving differences and institutionalizing best practices within the appropriate legal frameworks.

In terms of network defense—which is but one element of IO—I believe we have made tangible strides even in the past few years in bringing order and discipline to the DOD networks. My Joint Task Force Global Network Operations has made a measurable difference in the security and integrity of our DOD information systems, and the federal government has taken notice of our successes and regularly seeks our input on governance and security implementation measures.

Mr. THORNBERRY. You've mentioned your responsibility to protect the network as part of your Commander Joint Task Force-Global Network Operations. How does this work? In particular what do you do compared with Joint Functional Component Command-Network Warfare? Specifically how do the two organizations work together?

General CROOM. The Joint Task Force-Global Network Operations (JTF-GNO) has the responsibility to operate and defend the information infrastructure of the department. The JTF-GNO focuses on operational procedures and tools on ensuring the Department's information infrastructure is best poised to support the Department's missions. This means that customers can successfully execute their missions in spite of whatever is happening in the information infrastructure. For example, when we get a hint that something bad is or could be happening in the infrastructure, whether a cable cut, a computing failure, unexpected spikes in demand for a service, or a cyber attack, we start a triage and diagnosis process focused on determining what is really going on so that we can construct the most militarily appropriate reaction. In this diagnosis process we inform all parties we believe would be interested that something is going on, and we work with whatever partners are appropriate to the situation to do the diagnosis. This means we work with partners throughout the DOD, the intelligence community, our customer community, industry, and other parts of government.

The next phase of our response to an incident is the development of militarily useful courses of action, the selection of one of these, then the execution of the selection. Depending on the results of our diagnosis work, we may work closely with the Joint Functional Component Command-Network Warfare (JFCC-NW) in the development of courses of action since some potential actions may affect other information warfare missions, or since some of our possible courses of action may involve military capabilities and units that are not directly under my control as the Commander of the JTF-GNO. The JFCC-NW can bring these forces to bear on the situation, if necessary. We also work with other Combatant Commanders who may be affected by an incident, or who may have forces and capabilities necessary to appropriate reaction to the incident. Additionally, depending on the course of action selected, the JFCC-NW may be involved in coordinating part of the action, or involved in monitoring effectiveness of the action.

We also work closely with the JFCC-NW in deliberate planning, and in the deconfliction of other information operations missions that may be going on at any

particular time so that we can ensure the DOD's information infrastructure is poised to properly support these missions.

I believe all of these processes and the relationship are working well.

Mr. THORNBERRY. What grade (A–F) would you give to our ability to detect and react, in a timely fashion, to attempts by our adversaries to infiltrate DOD networks? What are we doing to improve our posture?

General CROOM. Congressman Thornberry, I am not satisfied with our efforts to date in the context of your question and I would only give us (myself included) a grade of "C."

This business of building information infrastructures that can best resist intrusions and attacks, can detect and diagnosis these quickly, can be operated to be resilient in the face of these, and can support militarily useful reactions to these incidents and attacks is a new area of warfare. Just like every other area of warfare, in which technology developments by one side have led to operational, technology, and organizational changes by the other side, we must now react to changes in our adversaries and potential adversaries capabilities and intent in the information space.

The thing that makes this area of warfighting different is the speed at which technology changes, and as a consequence, the speed at which our adversaries and our potential adversaries can develop new methods of exploiting and attacking our information and information infrastructure. The other thing that makes this area a challenge is the anonymity inherent in the current generation of technologies that make up cyber space.

Based on the current understanding by the United States of the capabilities and intent of our adversaries and potential adversaries, we have deployed and operate both commercial and government-developed methods of monitoring and diagnosis, and have procedures and tactics we use to do this that we practice. Owing to the difficulty of attribution, we also partner with the intelligence community in the diagnosis of certain probes, incidents, and attacks that originate offshore.

The Department has developed operational procedures for a range of reactions to incidents and attacks. These include a wide range of partners both within and outside the Department.

Additionally, the Department continuously re-evaluates our detection, diagnosis, and reaction capabilities, our resistance to exploitation and attack, and we work to adjust accordingly. We adjust our investments and recommended investments in protection, detection, and reaction technologies via the Global Information Grid portfolio management office, which is under the Assistant Secretary of Defense for Networks and Integrated Information. We adjust our operational procedures, training, and exercises, under my hat as the Commander of the Joint Task Force-Global Network Operations.

As a result of these efforts, we are always deploying improved protection, detection, and reaction technologies and operational procedures. For certain kinds of exploitation and attack we are good at detection and reaction, and we are getting better. For other kinds of exploitation and attack, we do not yet have the speed and diagnosis fidelity that I believe we need to ensure that we can react in militarily useful ways, and with militarily useful speed.

So, as the person responsible for operation and defense of the Department's information infrastructure, I am not yet satisfied at the resistance of our infrastructures to exploitation and attack, and I am not yet satisfied in my ability to detect, diagnose, develop militarily useful courses of action, and react to attacks. I am also not satisfied in my understanding of adversary and potential adversary capabilities and intent.

As I mentioned earlier, I see improvements in all of these areas. However, as the operational commander, I am also not yet satisfied that the pace of improvement will keep up with the pace of our adversaries and potential adversaries. We need better understanding of adversary capabilities and intent, and we need a more agile process for allocating resources to, then acquiring, developing, and fielding protection, detection/diagnosis, and reaction capabilities.

Mr. THORNBERRY. From press reporting, intrusions into the GIG and other DOD networks seem to be just against unclassified systems. Is there any indication that our classified networks have been penetrated? What is done to monitor those networks?

General CROOM. There is no indication that our classified networks have been penetrated. That said, the Department focuses a tremendous amount of attention on the hardening of these networks, on the monitoring for penetrations and other kinds of attack, and on practicing operational procedures for detecting and reacting to incidents and attacks on these networks. In addition to an array of protection mechanisms that include government-grade cryptography, the Department has de-

ployed, and is continuously improving, technologies and procedures for monitoring for anomalous behavior by insiders, for anomalous behavior of our systems, for monitoring for leaks from the classified networks, and for other sorts of things that the Department believes would be indicators of an exploit or attempted exploit.

I can say however, that just as on the unclassified networks, we have programs to constantly improve our resistance to attack, our ability to detect an attack, our operational procedures, and the training of our people.

Mr. THORNBERRY. During the hearing you mentioned that you believe you may lose a portion of the skilled work force due to an upcoming move to Fort George G. Meade, Maryland. What are your specific plans to assess the loss and develop plans to attract the talent you need to ensure DISA is still able to perform its mission?

General CROOM. DISA will be relocating 4,272 positions to Fort Meade, MD. Construction on a new facility at Fort Meade for the DISA workforce will begin in July, 2008. The projected timeline for completing the relocation of employees is July, 2011. More than 70% of the current workforce resides in Northern Virginia and more than 80% of the workforce is in technical or engineering/science positions with highly marketable skills.

DISA assesses the potential loss of personnel via regular surveys to determine employees' views on relocating and also solicit input on factors that may increase workforce interest in the relocation. DISA also has an on-going workforce planning process that assesses agency trends related to attrition, retirement eligibility, future skill gaps, and succession planning. One component of this plan is an aggressive Intern hiring program whereby the agency hires on average more than 100 recent college graduates and an additional 100 current college students per year to facilitate replenishing the talent within the agency. This program has resulted in reducing the average age of DISA's workforce to below the federal-wide average.

DISA also developed a comprehensive BRAC Human Resources (HR) Plan which outlines various incentives that will be available to relocating employees plus information on teleworking and other quality of life opportunities, housing, education, transportation, possible spouse employment, and many other initiatives. The BRAC HR Plan is updated regularly to add additional incentives/initiatives for both current and prospective employees and to adjust recruitment and retention strategies as necessary to ensure DISA is postured for the future.

○